LES 48 PREMIÈRES HEURES :

Réagir efficacement à une **fuite de données**

CYBERSCOUT® | Northbridge® Assurance

Combien de temps mettriez-vous à déceler une atteinte à la protection des données? Si certaines cyberattaques sont immédiatement détectables, beaucoup d'autres ne le sont pas. En fait, une récente étude estime le délai moyen pour découvrir une fuite à 197 jours, et il faut souvent plus de deux mois pour la colmater.

Supposons que vous avez découvert une violation des données. Que faites-vous ensuite? De bonnes mesures préventives peuvent vous aider à éviter la catastrophe, mais aucune entreprise n'est à l'abri d'une attaque soudaine. Un plan d'intervention réfléchi et éprouvé représente votre meilleure chance de limiter les dégâts.

En lisant ce rapport spécial, vous comprendrez mieux à quoi vous attendre durant les 48 premières heures suivant un incident. Vous découvrirez ce qu'un plan d'intervention peut apporter à votre entreprise, comment le préparer et le mettre à exécution, ainsi que les prochaines étapes vers le chemin du rétablissement. Ainsi, vous serez bien outillé pour élaborer un plan d'intervention clair, concis et pratique qui pourrait sauver votre entreprise durant et après une atteinte à la protection des données.

Économiser grâce à un plan d'intervention en cas d'atteinte à la protection des données 4

Votre plan d'intervention 5

Étape 1 : Limiter les dégâts 6
Étape 2 : Faire enquête 7
Étape 3 : Communiquer 9
Étape 4 : Restaurer 11

Tirer des leçons et planifier pour l'avenir 13

Comment Northbridge peut vous aider 15

Économiser grâce à un plan d'intervention en cas d'atteinte à la protection des données

Lorsqu'il y a violation de données, le temps, c'est de l'argent. En effet, réagir rapidement et efficacement s'avère souvent moins coûteux. Au bout du compte, vous pourriez rentabiliser votre investissement d'aujourd'hui dans un plan d'intervention solide à de multiples reprises au cours des prochaines années.

Un plan d'intervention bien pensé et éprouvé peut réduire les dépenses engagées dans la foulée d'un incident – et plus que vous le pensez. Une étude réalisée en 2018 par le Ponemon Institute indique que le déploiement d'une équipe d'intervention est particulièrement bénéfique pour les entreprises, leur faisant économiser 14 $ en moyenne par fichier compromis (sur un coût unitaire moyen de 148 $). Pourquoi? Parce que le processus d'enquête, les communications, les frais juridiques et les obligations réglementaires représentent une grande partie des coûts engagés après un incident.

Il n'y a pas que les experts externes qui peuvent jouer un rôle central dans votre plan d'intervention; votre propre personnel aussi. Réagir à un tel incident, et se rétablir après coup, est un véritable travail d'équipe, du début à la fin, et les deux premiers jours sont décisifs. En sachant ce qui vous attend, vous pourrez vous préparer beaucoup plus efficacement.

Votre plan d'intervention

Dès que vous soupçonnez une atteinte à la protection des données, il est temps d'agir. La prise de mesures judicieuses et calculées dans les heures suivant l'atteinte peut vous aider à limiter les dommages, à freiner les effets négatifs et à favoriser le rétablissement rapide et complet de votre entreprise.

Un plan d'intervention en cas d'atteinte à la protection des données comporte **quatre étapes clés**, mais chacune d'elle comprend de nombreux éléments. Vous devez donc pouvoir compter sur une équipe bien préparée. Plus vous avez d'alliés et plus leurs efforts sont coordonnés, meilleures sont vos chances d'éviter les dommages persistants à votre entreprise, à sa réputation et à sa rentabilité.

ÉTAPE 1 : LIMITER LES DÉGÂTS

Le mal est fait : il y a eu atteinte à la protection des données. La première chose à faire est de limiter les dégâts. Vous devez agir immédiatement en prenant des mesures liées aux TI, à la sécurité et au personnel.

À cette étape, vous devez accomplir trois tâches essentielles :

1. Protéger les métadonnées (c'est-à-dire les données qui fournissent de l'information sur les autres données).
2. Conserver, isoler et protéger les documents (pour ce faire, vous pouvez remplacer le disque dur des serveurs touchés).
3. Faire appel aux services d'un conseiller juridique.

Régler tout de suite les questions de responsabilité civile peut vous sembler un peu prématuré, mais il est important de faire part de la situation à un conseiller juridique le plus tôt possible. En cas de problème de confidentialité, cet expert vous aidera à protéger toute information découverte pendant cette étape et à empêcher sa divulgation.

En cas de problème de confidentialité, votre conseiller juridique vous aidera à protéger toute information découverte pendant cette étape et à empêcher sa divulgation.

ÉTAPE 2 : FAIRE ENQUÊTE

La prochaine étape est d'évaluer la situation, ce qui ne se fait pas en un clin d'œil. Vous devez rassembler des renseignements sur la nature des fichiers touchés et la façon dont ils ont été compromis. Tâchez de ne pas sauter aux conclusions.

Quelles données ont été compromises?

Vous devez savoir quelles données ont été compromises afin d'évaluer l'ampleur du problème, mais aussi de déterminer si vous avez l'obligation de notifier vos clients et vos employés. S'il s'agit de coordonnées (ex. : nom ou adresse), vous n'êtes peut-être pas obligé d'informer qui que ce soit; toutefois, s'il s'agit de données de nature sensible (ex. : numéros d'assurance sociale ou numéros de compte), les personnes concernées courent de plus grands risques, et vous devriez prendre le tout très au sérieux.

Comment l'incident s'est-il produit?

Hameçonnage. Piratage. Piratage psychologique. Ces types d'attaques font régulièrement la manchette, bien qu'elles ne soient pas à l'origine de toutes les violations de données. L'infonuagique est généralement considérée comme étant une technologie plus sûre en ce qui concerne les cyberrisques, mais elle n'est pas infaillible : bien que les fournisseurs de tels services respectent certaines normes de sécurité, celles-ci ne répondent pas forcément aux besoins en matière de sécurité des entreprises canadiennes.

Même un employé bien intentionné peut commettre une erreur. Il suffit d'un ordinateur portable laissé au mauvais endroit, d'un mot de passe un peu faible ou de l'ouverture d'une pièce jointe en apparence légitime. D'autres fois, une cyberattaque est causée par une personne mal intentionnée, comme un employé rancunier ou opportuniste qui aurait installé des enregistreurs de frappe sur vos ordinateurs pour recueillir des dizaines de mots de passe. Il est important que vous réfléchissiez à toutes les causes possibles derrière une atteinte.

Pouvez-vous régler le problème vous-même?

Une fois que vous avez déterminé la nature et l'ampleur de l'incident, vous pouvez décider de la marche à suivre.

Le rôle de votre service des TI variera en fonction de la cause de l'incident. Par exemple, s'il s'agit d'une erreur humaine, accidentelle ou délibérée, la priorité de vos experts des TI sera sans doute de :

- déterminer quelles données ont été volées ou compromises;
- consigner les détails techniques de l'incident.

Si la cause est plutôt d'ordre technologique, votre équipe des TI s'efforcera également de colmater la fuite de données. Pour ce faire, elle aura peut-être besoin des services d'un spécialiste de l'informatique judiciaire, qui pourra passer au crible votre infrastructure technologique et ainsi libérer vos équipes internes afin qu'elles puissent se concentrer sur vos systèmes de sécurité critiques.

Faites preuve de sang-froid et de discrétion

Vous pensez avoir mis le doigt sur la cause du problème? Arrêtez-vous un instant, et n'agissez pas impulsivement. En fermant un serveur infecté, vous pourriez détruire de précieuses preuves. De plus, congédier un employé malveillant pourrait affaiblir votre dossier pendant l'enquête.

Il est parfois préférable de laisser l'incident suivre son cours, et de surveiller de près l'extraction et l'utilisation de vos données. Cette attitude passive vous permettra de vous rétablir plus rapidement et d'informer les personnes qui doivent l'être. Toutefois, cette approche n'est pas une solution universelle. Si vous êtes victime d'un rançongiciel, vous feriez probablement mieux de déconnecter immédiatement votre réseau et de tenter de restaurer vos copies de sauvegarde. Vous n'êtes pas certain de la méthode à adopter? Vos spécialistes de la cybersécurité et votre conseiller juridique vous aideront à décider de la meilleure approche, alors n'hésitez pas à leur demander conseil avant de faire appel à quelqu'un d'autre.

Protégez vos données privilégiées

Votre conseiller juridique sera l'un de vos plus importants alliés pendant les premières étapes de la réponse à l'incident. Après tout, c'est lui qui peut vous aider à protéger l'information privilégiée révélée par l'enquête, ainsi qu'à mettre au fait les personnes concernées.

Vous devrez peut-être avoir recours aux services d'experts juridiques internes et externes pour réagir à une atteinte à la protection de données de nature sensible. Vos conseillers internes connaissent bien votre entreprise, mais ils auront peut-être besoin d'une expertise venant de l'extérieur pour les questions de confidentialité et de réglementation.

Une équipe constituée d'experts juridiques internes et externes pourrait se révéler utile, surtout si les experts externes ont l'habitude des problèmes liés à la cybersécurité et à la confidentialité, et qu'ils connaissent bien les différentes assurances et exigences réglementaires.

Vous n'êtes pas certain de la méthode à adopter? Vos spécialistes de la cybersécurité et votre conseiller juridique vous aideront à décider de la meilleure approche, alors n'hésitez pas à leur demander conseil avant de faire appel à quelqu'un d'autre.

ÉTAPE 3 : COMMUNIQUER

Votre équipe juridique jouera un grand rôle dans la communication de l'étendue et des conséquences de la brèche de sécurité, notamment des obligations légales à respecter. Toutefois, d'autres employés importants doivent aussi vous aider à diffuser l'information essentielle et à transmettre les avis après la fuite.

Répondre adéquatement à une atteinte à la protection des données peut prendre des semaines, voire des mois. Si vous ne pouvez pas justifier le fait de détourner vos employés de leurs tâches productives afin qu'ils puissent se concentrer sur l'incident, vous devriez faire appel à des spécialistes externes en gestion des atteintes qui pourront s'occuper des tâches supplémentaires et simplifier votre plan d'intervention grâce à leur solide expérience.

Évaluez le risque de préjudice grave

À compter du 1er novembre 2018, la Loi sur la protection des renseignements personnels et les documents électroniques du gouvernement fédéral canadien obligera les entreprises à informer les personnes et entreprises touchées par une atteinte qui courent un risque réel de préjudice grave. L'incident devra aussi être signalé au commissaire à la protection de la vie privée du Canada, et un registre des atteintes devra être tenu.

Cette loi rend plus important que jamais pour les entreprises de déterminer leurs obligations juridiques à l'égard de l'évaluation du risque de préjudice grave. S'il n'y a pas de risque, il n'est pas obligatoire d'informer qui que ce soit, mais vous ne pouvez pas présumer que c'est le cas sans une évaluation attentive.

Communications externes

Votre équipe des relations publiques peut recueillir des renseignements sur l'ampleur de la fuite auprès de l'équipe de la sécurité de l'information ou de l'informatique judiciaire, et collaborer avec les conseillers juridiques pour rédiger un message approprié à l'intention du public. À l'instar des conseillers juridiques, votre équipe des relations publiques pourrait s'allier à des experts externes pour bien couvrir vos arrières.

À quel point votre équipe des relations publiques est-elle familiarisée avec la communication en situation de crise? Peut-elle se permettre de mettre

de côté certaines de ses tâches quotidiennes – et si oui, lesquelles – pour s'occuper de la gestion de crise? À moins que votre équipe interne n'ait déjà mis au point un plan de communication clair et détaillé pour ce genre d'incident, vous devriez penser à recourir aux services d'un cabinet de relations publiques expérimenté pour vous aider à gérer le volet communication et à limiter les dommages à votre réputation. Ce cabinet pourrait aussi vous guider en ce qui a trait à votre réponse aux médias ou à tout message pertinent à diffuser après coup.

Communications internes

Si votre équipe des relations publiques s'occupe des communications externes, celle des ressources humaines supervise quant à elle la communication avec vos employés. Elle devrait donc être mise au fait de l'évolution de la situation. De son côté, votre équipe des relations publiques peut aider à préparer les principaux messages à transmettre aux employés par l'équipe des ressources humaines.

Si vous possédez une grande entreprise, votre équipe des ressources humaines interne ne pourra peut-être pas s'occuper de tout ce surcroît de travail. Si les questions d'employés affluent en trop grand nombre, vous pourriez mandater un centre d'appels externe pour agir à titre de première ligne. Les employés qui ne sont pas satisfaits des réponses toutes faites peuvent être dirigés vers votre service des RH pour obtenir des réponses plus personnalisées.

Informez les administrateurs, les organismes de réglementation et les intervenants

Vos équipes des relations publiques, des TI et des services juridiques doivent transmettre l'information rendue publique aux membres de votre conseil d'administration, et les tenir informés de l'évolution de la situation et des plans de communication par des mises à jour régulières. Une fois votre conseil d'administration informé de la façon de répondre aux questions des médias, vous serez certain que tout le monde est sur la même longueur d'onde.

Si vous avez déterminé qu'il existe un risque réel de préjudice grave, vous devez en aviser les personnes et entreprises concernées, y compris le commissaire à la protection de la vie privée, ce qui pourrait entraîner des coûts supplémentaires. Enfin, puisque certaines dépenses imprévues pourraient toucher vos intervenants, vous devez aussi informer ces derniers de la situation.

Les membres de votre conseil d'administration ont peut-être une assurance de la responsabilité civile pour couvrir les coûts des poursuites. Vous devriez consulter votre équipe juridique pour savoir si vous disposez d'une assurance qui pourrait intervenir après l'incident.

Qui dirige?

Quelqu'un doit rester à la barre pendant toute la durée de la réponse à l'incident. Qui sera l'heureux élu? Gérer l'ensemble de la procédure est une grande responsabilité, car la situation peut prendre des semaines ou même des mois avant d'être résolue. Souvent, vous pourrez limiter l'incidence sur votre entreprise et vos clients en laissant vos employés s'occuper de leurs tâches habituelles; nommez donc d'emblée un responsable de l'intervention et tenez-vous-en à la structure de soutien interne et externe déjà en place.

ÉTAPE 4 : RESTAURER

Après avoir pris la mesure de la situation et mis fin à toute fuite de données, vous pourrez vous concentrer sur votre rétablissement, ce qui passe par la récupération des données perdues, la prévention des pertes futures et la compréhension des différentes répercussions de l'incident.

Vous devrez maintenant agir pour :

- récupérer vos données;
- prévenir la divulgation d'autres données.

En règle générale, vous aurez besoin des conseils d'un expert et d'une aide pratique.

Proposez des services de surveillance du crédit

Offrir des services de surveillance du crédit aux parties potentiellement touchées est une pratique courante, et un gage de bonne foi. Les entreprises qui facilitent l'accès à un tel service après une atteinte à la protection des données contribuent également à se constituer une défense qui pourra être mise à profit en cas de poursuite. En effet, savoir qui a été touché financièrement lors de l'incident permettra de déterminer plus précisément l'ampleur des dommages.

Choisissez judicieusement vos partenaires pour votre rétablissement

Les atteintes à la protection des données peuvent s'avérer complexes à résoudre, et vous n'avez pas à porter ce fardeau seul. Toutefois, faites preuve de jugement dans le choix de vos partenaires. Prenez le temps de trouver les bons alliés qui vous aideront à éviter les problèmes futurs, à gérer les contrecoups avec efficacité et à remettre votre entreprise sur les rails le plus vite possible.

Si vous décidez de faire appel à des fournisseurs pour vos efforts de reprise, résistez à la tentation de choisir le premier venu. Avant d'accepter l'aide d'un fournisseur, demandez-lui plus de détails sur

son expérience avec le type d'attaque dont vous êtes victime en lui posant des questions comme celles-ci :

- Combien d'atteintes à la protection des données avez-vous résolues?
- Quelle était leur gravité?
- Collaborez-vous avec des compagnies d'assurance?
- Offrez-vous une gamme de services à la carte ou un forfait tout inclus?
- En quoi consistent vos processus et vos conditions contractuelles?

Certains fournisseurs imposent un montant minimum par incident, et vous vous retrouveriez peut-être à payer plus cher pour rien. Par conséquent, il est important de clarifier les conditions et les obligations mutuelles avant de signer quoi que ce soit.

Un plan en cas de litige

L'identité des personnes à aviser de l'incident est peut-être régie par la loi; il serait donc judicieux de vous en assurer avant tout afin que vous sachiez ce qu'on attendra de vous une fois que vous aurez signalé l'incident aux autorités.

Malheureusement, les déboires juridiques sont monnaie courante après une atteinte à la protection des données, et ils peuvent être éprouvants et coûteux pour votre entreprise. Élaborez un plan d'intervention en cas de poursuite; c'est à ce moment que la bonne assurance des entreprises pourrait vous sauver la mise en allégeant un peu le fardeau financier qui pourrait fortement ébranler votre entreprise.

Certains fournisseurs imposent un montant minimum par incident, et vous vous retrouveriez peut-être à payer plus cher pour rien. Par conséquent, il est important de clarifier les conditions et les obligations mutuelles avant de signer quoi que ce soit.

Tirer des leçons et planifier pour l'avenir

Attention! Les cybermenaces persistent, évoluent et se transforment. Il est presque impossible d'affirmer à coup sûr que votre entreprise est à l'abri d'un nouvel incident, et ce, peu importe la quantité de ressources déployées ou l'efficacité de votre réponse coordonnée; même le géant Bell Canada a subi deux fuites de données en l'espace d'un an.

Toutefois, en tirant des leçons et en modifiant votre routine en conséquence, vous pourrez réduire les risques d'une nouvelle fuite.

Les souvenirs s'estompent, les écrits restent – tenez un registre

Consigner les détails de l'incident vous aide à savoir comment réagir en cas d'audit, de plainte ou d'enquête. Comme il n'y a pas de consensus sur la définition d'une atteinte et la marche à suivre pour y répondre, vous devrez expliquer votre processus, votre analyse et votre raisonnement si jamais vous deviez défendre vos actions.

Processus

Dès le début de votre enquête, établissez la chronologie des événements. Un récit chronologique des faits vous permettra de décrire ce qui s'est passé, et à quel moment,

ce qui pourrait s'avérer utile si jamais la mémoire vous faisait défaut. Pensez à consigner tous les détails, y compris les transcriptions des premiers appels internes.

Votre équipe de la sécurité de l'information peut déterminer la nature des données compromises et l'ampleur de l'incident. Consignez toutes les décisions prises par le soutien technique, et ses actions, dans une annexe jointe au compte rendu.

Analyse

Après avoir évalué l'ampleur de l'incident et déterminé toutes les exigences à respecter en matière d'avis, racontez exactement ce qui s'est passé, la façon dont vous avez réagi et pourquoi. De cette façon, tous les détails de votre réponse à l'incident seront clairs s'il vous fallait revoir ce dossier un jour.

Raisonnement

En plus d'évaluer l'exposition aux risques, rassemblez toutes vos réflexions à cet égard dans un rapport clair et concis. À quel genre de préjudice vos clients ou vos employés auraient-ils pu être exposés? Si vous faites l'objet d'un audit ou d'une enquête d'un organisme de réglementation, vous pourrez prouver tous les efforts déployés pour déterminer l'incidence de la fuite sur vos clients et vos employés, ainsi que toutes les mesures prises pour informer les différentes personnes touchées et résoudre le problème.

Renforcez la sécurité de votre entreprise

C'est terminé! Vous avez mené à bien votre intervention, et vous êtes maintenant prêt à reprendre le cours normal de vos activités. Il s'agit du moment idéal pour vous assurer que les activités de votre entreprise sont en règle, et que ses dispositifs de sécurité respectent les exigences en la matière. Mettez à l'épreuve vos mesures de sécurité contre les nouvelles cybermenaces au moins une fois par trimestre en :

- tenant à jour vos systèmes et vos logiciels au moyen des plus récents correctifs de sécurité;
- faisant appel à une entreprise externe qui pourra procéder à un test d'intrusion et simuler une attaque contre votre système; en fonction des résultats, ils formuleront des recommandations pour en corriger les faiblesses.

Concentrez-vous sur vos employés

Vos employés représentent peut-être le maillon faible de votre entreprise – ou votre première ligne de défense. Prenez le temps de former vos employés, et ce, continuellement. En effet, la formation doit se faire en continu, car une seule séance n'est pas suffisante pour s'assurer d'avoir un effectif avisé en matière de cybersécurité.

Tenez vos employés au fait des risques, informez-les des attentes relatives à la sécurité et mettez en pratique votre plan d'intervention en simulant différents scénarios. Voici quelques-unes des meilleures pratiques qui aideront vos employés à protéger votre entreprise :

- Créer une plateforme de formation en ligne comprenant des modules d'apprentissage adaptés à votre secteur.
- Suivre les progrès de vos employés (à titre de référence interne et pour les audits externes).
- Encourager vos employés à créer des mots de passe forts et uniques et leur rappeler de les changer régulièrement.
- Exercer vos employés à reconnaître les tentatives d'hameçonnage.
- Vous exercer encore et encore; simuler une atteinte à la protection des données peut vous aider à vous assurer que l'équipe comprend bien votre plan d'intervention et qu'elle est prête à réagir au quart de tour.

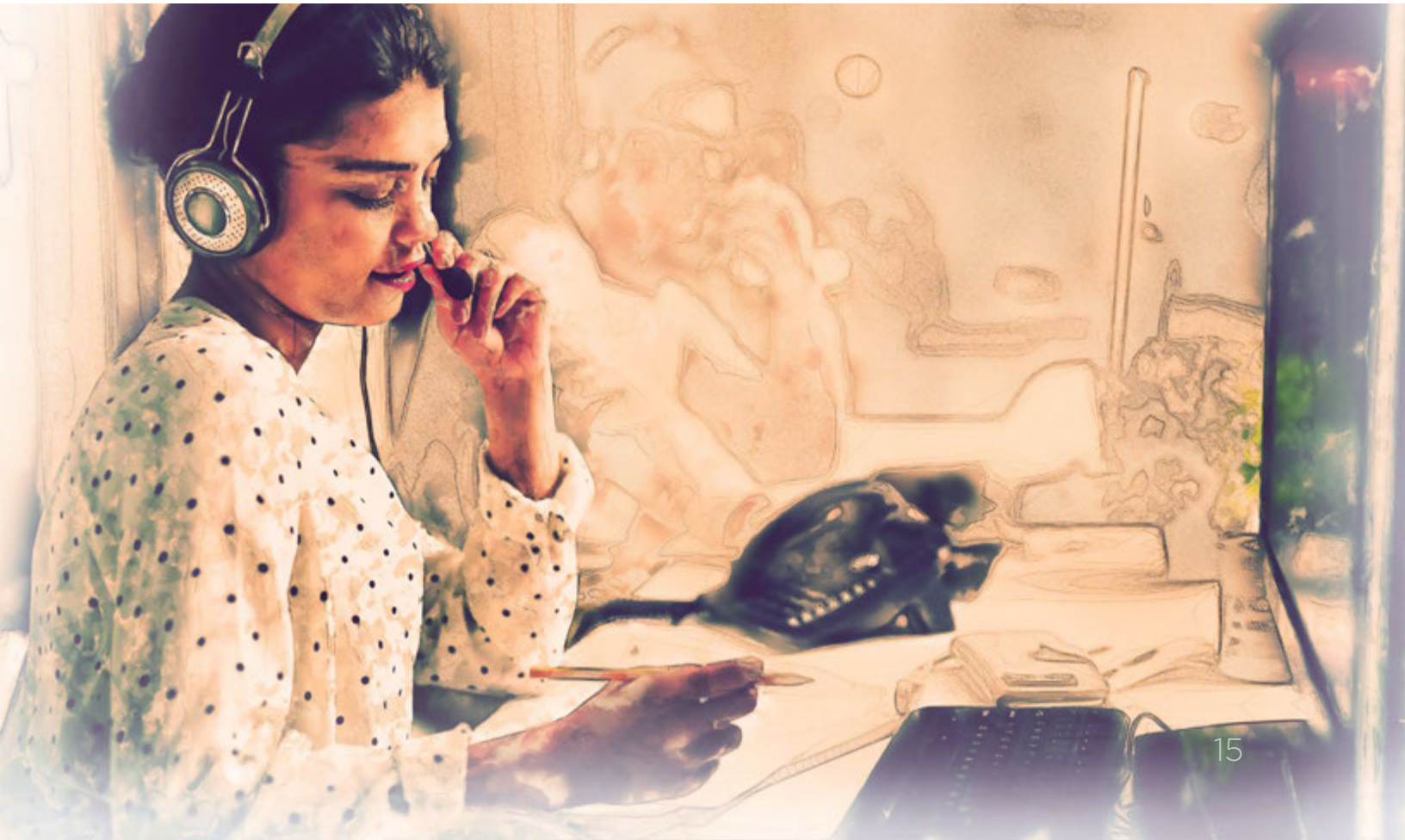
Faites également attention de ne pas commettre certaines erreurs typiques qui nuiront à vos efforts d'amélioration. Les cours magistraux sont parfois assez arides et peinent à accrocher l'attention des participants, ce qui ne vous aidera pas vraiment à préparer vos employés à faire face à une situation de crise. De plus, n'oubliez pas d'évaluer la compréhension et la vigilance de vos employés. Réservez un moment pour vous assurer qu'ils connaissent votre plan de fond en comble et le rôle qu'ils jouent dans celui-ci.

Comment Northbridge peut vous aider

Il est normal de commettre des erreurs de temps en temps, et les cybercriminels ne cesseront certainement pas de trouver de nouvelles façons d'exploiter les données de votre entreprise. Bien qu'il soit important de protéger votre entreprise autant que possible, la bonne assurance pourrait venir à votre rescousse si vos efforts ne s'avéraient pas suffisants.

Les assurances des cyberrisques ne sont pas toutes pareilles. Sans une assurance adaptée à votre situation, vous pourriez devoir assumer les frais juridiques, les amendes, les coûts de réparation et les frais de reprise des activités résultant d'un incident majeur. De plus, les rançongiciels, les maliciels et autres attaques ciblées étant devenus plus complexes et généralisés, une seule attaque du genre pourrait vous causer d'importants problèmes financiers.

En partenariat avec CyberScout, Northbridge Assurance a mis au point l'Assurance des cyberrisques, un produit d'assurance polyvalent. En plus de protéger vos finances en cas de fuite, votre police vous donne accès à des cyberressources complètes, à une aide réactive et à des conseils personnalisés pour veiller à ce que ce genre d'incident ne se reproduise jamais. Après tout, la gestion des risques s'exerce en continu, et Northbridge prend cette gestion très au sérieux, notamment en vous offrant des polices complètes qui placent la réussite à long terme de votre entreprise au centre des priorités.



Northbridge Assurance | CYBERSCOUT®