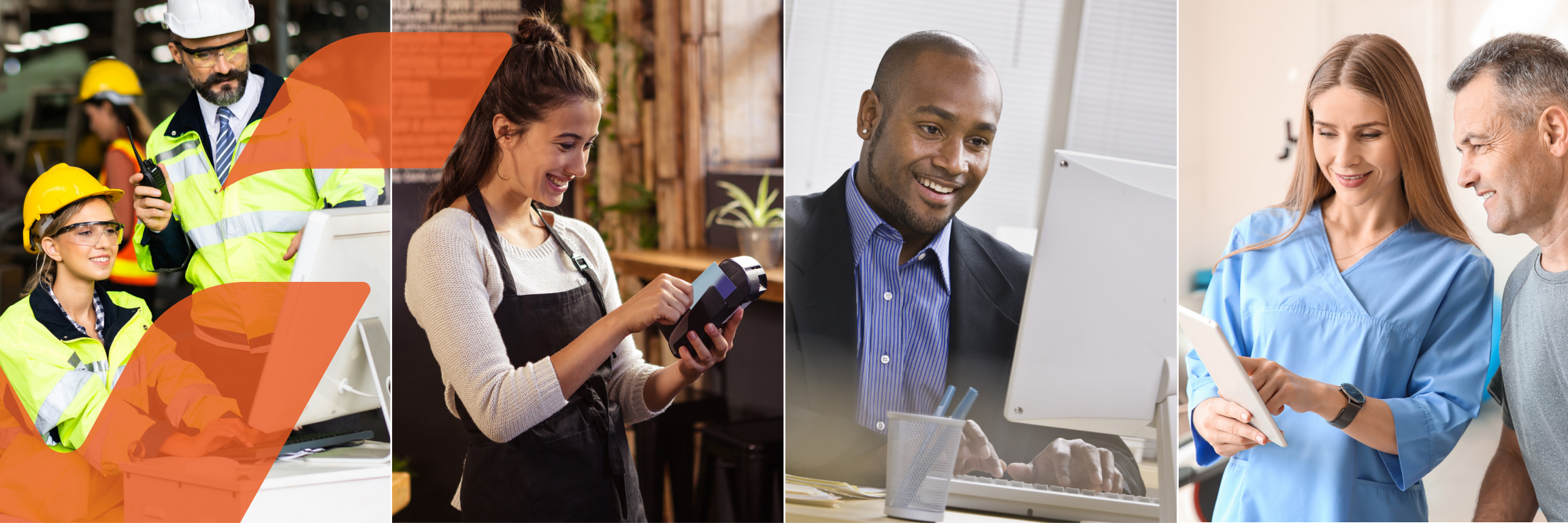
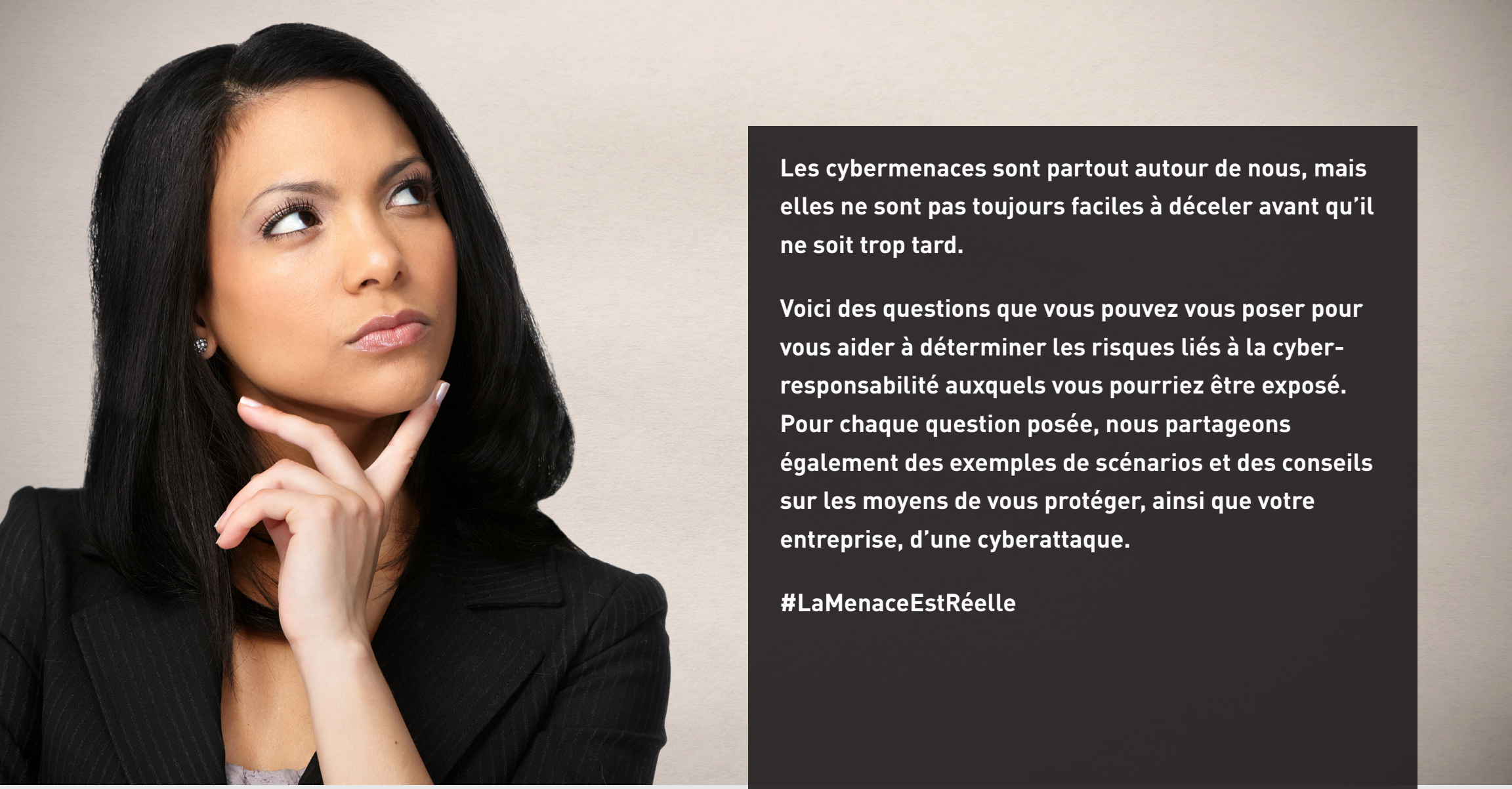


Risques liés à la cyber-responsabilité

Comment vous protéger, ainsi que votre entreprise

VICTOR



Les cybermenaces sont partout autour de nous, mais elles ne sont pas toujours faciles à déceler avant qu'il ne soit trop tard.

Voici des questions que vous pouvez vous poser pour vous aider à déterminer les risques liés à la cyber-responsabilité auxquels vous pourriez être exposé. Pour chaque question posée, nous partageons également des exemples de scénarios et des conseils sur les moyens de vous protéger, ainsi que votre entreprise, d'une cyberattaque.

#LaMenaceEstRéelle

1. Utilisez-vous des ordinateurs, des réseaux ou des appareils mobiles?

Si tel est le cas, en cas de cyberattaque, voici quelques-unes des risques auxquelles vous pourriez être exposé :

Coûts d'extorsion et perte d'exploitation

Exemple de scénario

Un pirate informatique trouve un moyen d'accéder à votre ordinateur et à vos renseignements personnels, rendant ainsi votre ordinateur inutilisable. Le pirate informatique détient également vos renseignements personnels en otage, ce qui vous laisse complètement perdu et à la merci de celui-ci. Vos renseignements sont totalement inaccessibles et inutilisables.

Conseil

En tant que protection supplémentaire contre les pirates informatiques, assurez-vous de chiffrer vos données sensibles (c'est-à-dire, des renseignements confidentiels ou personnels) et d'avoir une protection de sécurité en place comme des pare-feu, des logiciels de détection d'intrusion, un antivirus et un antivol pour votre ordinateur ou tout appareil technologique. Effectuez des audits périodiques pour tester et analyser les vulnérabilités du système. Mettez en place un plan complet d'intervention en cas d'incident pour remédier à l'atteinte et atténuer ses répercussions sur votre entreprise. Utilisez un Wi-Fi sécurisé; n'utilisez pas de Wi-Fi ouvert ou accessible au public, car cela vous rend vulnérable aux pirates informatiques. N'oubliez pas de mettre en pratique des protocoles de sauvegarde réguliers (c'est-à-dire enregistrer vos fichiers sur un autre lecteur sécurisé et à distance) afin de ne pas vous retrouver dans une situation de perte complète en cas de cyberattaque.

Systèmes d'ingénierie sociale

Exemple de scénario

Un intervenant malhonnête réussit à tromper et à divulguer publiquement des renseignements sensibles sur vous et votre entreprise, causant ainsi une perte financière pour vous et votre entreprise.

Conseil

Assurez-vous que vous et les employés de votre entreprise êtes au courant des cybermenaces. Mettez en place des protocoles de sécurité solides pour lutter contre et prévenir les stratagèmes frauduleux qui pourraient être perpétrés contre vous et votre entreprise. Effectuez des simulations d'hameçonnage périodiques pour tester et évaluer les risques cybernétiques de votre organisation et les vulnérabilités aux cyberattaques. Les employés sont la meilleure ligne de défense en matière de protection contre les cyberattaques. La sensibilisation et la formation sont des facteurs clés pour aider à atténuer cette menace.

Atteinte à la réputation

Exemple de scénario

Votre réputation et celle de votre entreprise sont menacées par une cyberattaque. Vos clients perdent confiance en vous et en votre entreprise. La cyberattaque entraîne également une perte de revenus et de confiance dans la marque de votre entreprise.

Conseil

Soyez proactif dans la protection des renseignements confidentiels ou sensibles, surtout lorsque ces renseignements sont sous votre responsabilité. N'attendez pas une revendication pour mettre en œuvre les protocoles de sécurité appropriés. La prévention aidera à atténuer les impacts potentiels et dévastateurs sur votre réputation et votre viabilité globale. Assurez-vous que les renseignements sensibles stockés sur votre ordinateur et vos systèmes sont bien protégés grâce à un logiciel de chiffrement et de protection de la sécurité. Faites des audits périodiques et des évaluations de vulnérabilité. Si vous êtes sujet à une atteinte à la sécurité ou à la protection des renseignements personnels, consultez des experts comme un conseiller en cas d'atteintes cybernétiques et un professionnel des relations publiques. Un conseiller en cas d'atteintes cybernétiques peut vous orienter à travers l'atteinte cybernétique tandis que le professionnel des relations publiques peut vous aider à atténuer l'impact des atteintes potentielles à la réputation de votre entreprise.

2. Faites-vous la collecte ou le stockage de renseignements confidentiels ou personnels (ou quelqu'un le fait-il pour vous)?

Si tel est le cas, en cas de cyberattaque, voici les risques auxquels vous pourriez être exposé :

Amendes et pénalités réglementaires en matière de protection des renseignements personnels

Exemple de scénario

Vous êtes tenu responsable d'une violation des lois sur la protection des renseignements personnels au Canada aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Vous pourriez être condamné à une amende maximale de 100 000 $ CAN en raison d'atteinte à la protection des renseignements personnels.

Conseil

Pour votre entreprise, vous devez être au courant des différentes lois sur la protection des renseignements personnels où vous exercez et où se trouvent vos clients. Faites appel à un conseiller juridique spécialisé dans les lois sur la cybersécurité et la protection des données. Ils peuvent vous aider à vous assurer que vous répondez aux exigences minimales et à l'obligation de diligence envers vos clients et les organismes de réglementation. Cela atténuera le risque de réclamations ou d'amendes coûteuses en cas d'atteinte à la protection des renseignements personnels.

Atteinte à la protection des renseignements personnels

Exemple de scénario

Une atteinte à la protection des renseignements personnels se produit dans votre organisation. Un pirate informatique a eu accès aux renseignements confidentiels des clients. Vous faites face à des amendes réglementaires et à des réclamations coûteuses de tierces parties. Et, même si les renseignements confidentiels sur les clients sont gérés par quelqu'un d'autre en votre nom, cela ne vous a pas libéré de vos obligations envers vos clients. Vous pourriez envisager des dépenses supplémentaires comme les frais de notification aux personnes et aux organismes gouvernementaux concernés, les frais juridiques, les frais d'expertise médico-légale, les frais de consultation en relations publiques et en surveillance du crédit ainsi que les frais découlant d'un vol d'identité en raison de l'atteinte à la protection des renseignements personnels. De plus, vous devrez peut-être faire des heures supplémentaires et engager des dépenses comme l'embauche d'un centre d'appels pour régler l'atteinte à la protection des renseignements personnels.

Conseil

Assurez-vous d'avoir des protocoles sécurisés en place pour protéger et éliminer correctement les renseignements confidentiels ou personnels. Cela comprend le chiffrement de ces renseignements et l'accès à ces renseignements limité aux personnes autorisées, comme première étape. Utilisez une application de protection de sécurité et assurez-vous qu'elle est à jour. Testez régulièrement votre ordinateur et vos systèmes contre les vulnérabilités. Mettez en œuvre un plan de reprise des activités, de continuité des activités et de réaction aux incidents en cas d'atteinte à la protection des renseignements personnels. Assurez-vous également que vous et les employés de votre organisation êtes correctement formés aux protocoles de protection des renseignements personnels et de sécurité. Envisagez de consulter une firme de cybersécurité pour vous aider à déterminer vos vulnérabilités. Mettez en œuvre un plan de cybersécurité solide avec des protocoles de sécurité en place.

Amendes et pénalités de l'industrie des cartes de paiement (PCI)

Exemple de scénario

Votre entreprise traite des cartes de crédit. Ce faisant, votre entreprise enfreint les normes de sécurité PCI parce que vous n'avez pas protégé les renseignements confidentiels ou personnels des titulaires de carte. Cette violation donne lieu à des poursuites et des demandes de la part des institutions financières, des associations de cartes de crédit et des sociétés de traitement des cartes de paiement. Vous pourriez devoir payer des amendes et des évaluations coûteuses aux termes d'une entente de services aux commerçants.

Conseil

Si vous traitez des cartes de crédit pour votre entreprise, assurez-vous de respecter les normes de sécurité PCI. Cela comprend la protection des renseignements confidentiels ou personnels des titulaires de carte dont vous avez la garde et le respect de bonnes pratiques de protocole de sécurité (également mentionné précédemment comme un conseil dans la section **Atteinte à la protection des renseignements personnels**).

3. Traitez-vous des fonds par voie électronique?

Si tel est le cas, en cas de cyberattaque, voici les risques auxquels vous pourriez être exposé :

Traitement électronique des fonds

Exemple de scénario

Dans le traitement électronique des fonds par votre entreprise, les renseignements d'un client sont compromis par des intervenants malhonnêtes. Cela pourrait désormais entraîner des pertes financières si les renseignements de votre client contenaient des renseignements de carte de crédit ou bancaires. Les renseignements compromis, qui sont désormais entre les mains d'intervenants malhonnêtes, pourraient également exposer votre client au vol d'identité. En conséquence, votre réputation et celle de votre entreprise pourraient en souffrir. Vous pourriez être exposé à des réclamations coûteuses si votre client prétend avoir subi des dommages en raison de votre négligence à permettre la cyberattaque.

Conseil

Idéalement, utilisez une plateforme de commerce électronique de confiance qui garantira que les protections de sécurité appropriées sont en place et que des évaluations et une surveillance continues de la sécurité et des vulnérabilités sont menées dans votre entreprise. Utilisez HTTP avec SSL (couche de sockets sécurisés) pour votre plateforme Web pour vous assurer que le lien est chiffré entre le serveur Web et les navigateurs. Cela contribuera également à garantir que les renseignements sensibles, financiers et confidentiels que vous stockez numériquement dans vos systèmes informatiques restent privés et sécurisés. Enfin, assurez-vous que vous êtes conforme à la Norme de sécurité de l'industrie des cartes de paiement. Maintenez le site Web de votre entreprise à jour avec les applications et les correctifs les plus récents pour lutter contre les cyberattaques potentielles.

4. Avez-vous un site Web, un compte sur les réseaux sociaux ou faites-vous de la publicité publique?

Si tel est le cas, en cas de cyberattaque, voici les risques auxquels vous pourriez être exposé :

Diffamation

Exemple de scénario

Vous êtes exposé à des réclamations pour préjudice personnel parce que votre site Web, vos médias sociaux et votre contenu publicitaire font la promotion de fausses vérités présumées, des commentaires diffamatoires ou révèlent des renseignements sensibles.

Conseil

Assurez-vous d'obtenir les autorisations appropriées de tiers avant de communiquer des renseignements sur eux ou leur entreprise, y compris des logos ou des photos de leurs produits ou services. Communiquez des faits et évitez les opinions biaisées qui pourraient être considérées comme diffamatoires, ce qui pourrait également nuire à votre réputation et à celle de votre entreprise.

Violation

Exemple de scénario

Vous utilisez de manière inappropriée les droits d'auteur de quelqu'un d'autre, tels que des images, un logo ou du texte, sans sa permission.

Conseil

Effectuez toujours des recherches appropriées pour éviter toute violation lors du développement de produits, y compris des moyens de communication tels que des sites Web. Cela comprend également la réalisation de recherches appropriées lors de la création et du partage public de documents imprimés et numériques. N'oubliez pas d'obtenir la permission de tiers avant d'utiliser leurs renseignements exclusifs.

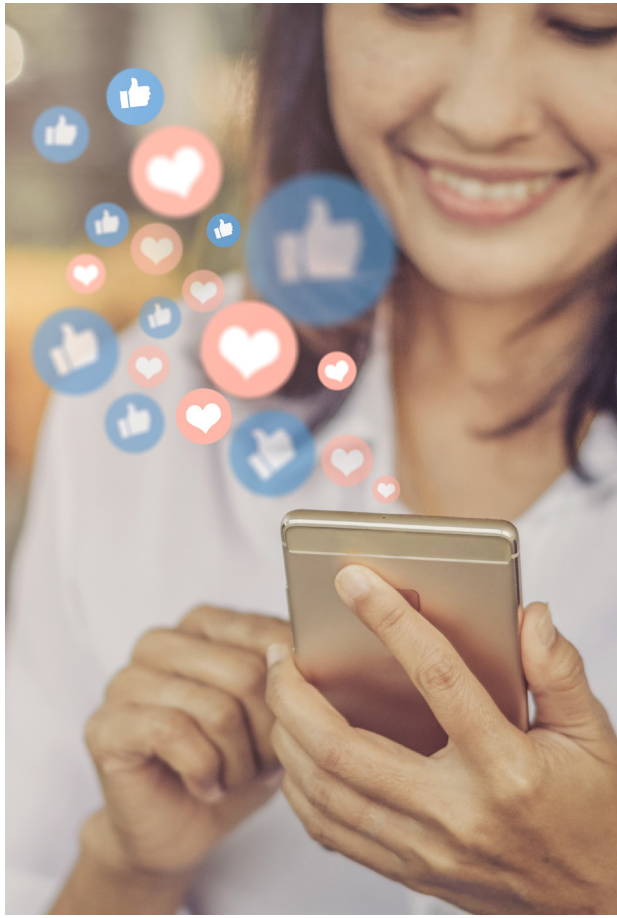
Vol ou fraude électronique

Exemple de scénario

Un pirate informatique ou un escroc utilise votre site Web et vos comptes de médias sociaux pour essayer de voler des fonds et potentiellement vous frauder, vous et vos clients. Le pirate informatique envoie un courriel à vos clients en prétendant être vous et demande des fonds en retour de vos services professionnels. Votre client paie le pirate informatique (en pensant que c'est vous). Votre client ne reçoit jamais vos services professionnels.

Conseil

Protégez-vous et méfiez-vous des messages par courriel de la part d'expéditeurs inconnus ou suspects. Ne cliquez sur aucun lien, sauf si vous avez une base raisonnable pour lui faire confiance, ou si le courriel provient d'une organisation bien établie.



5. Avez-vous des employés?

Si tel est le cas, en cas de cyberattaque, voici les risques auxquels vous pourriez être exposé :

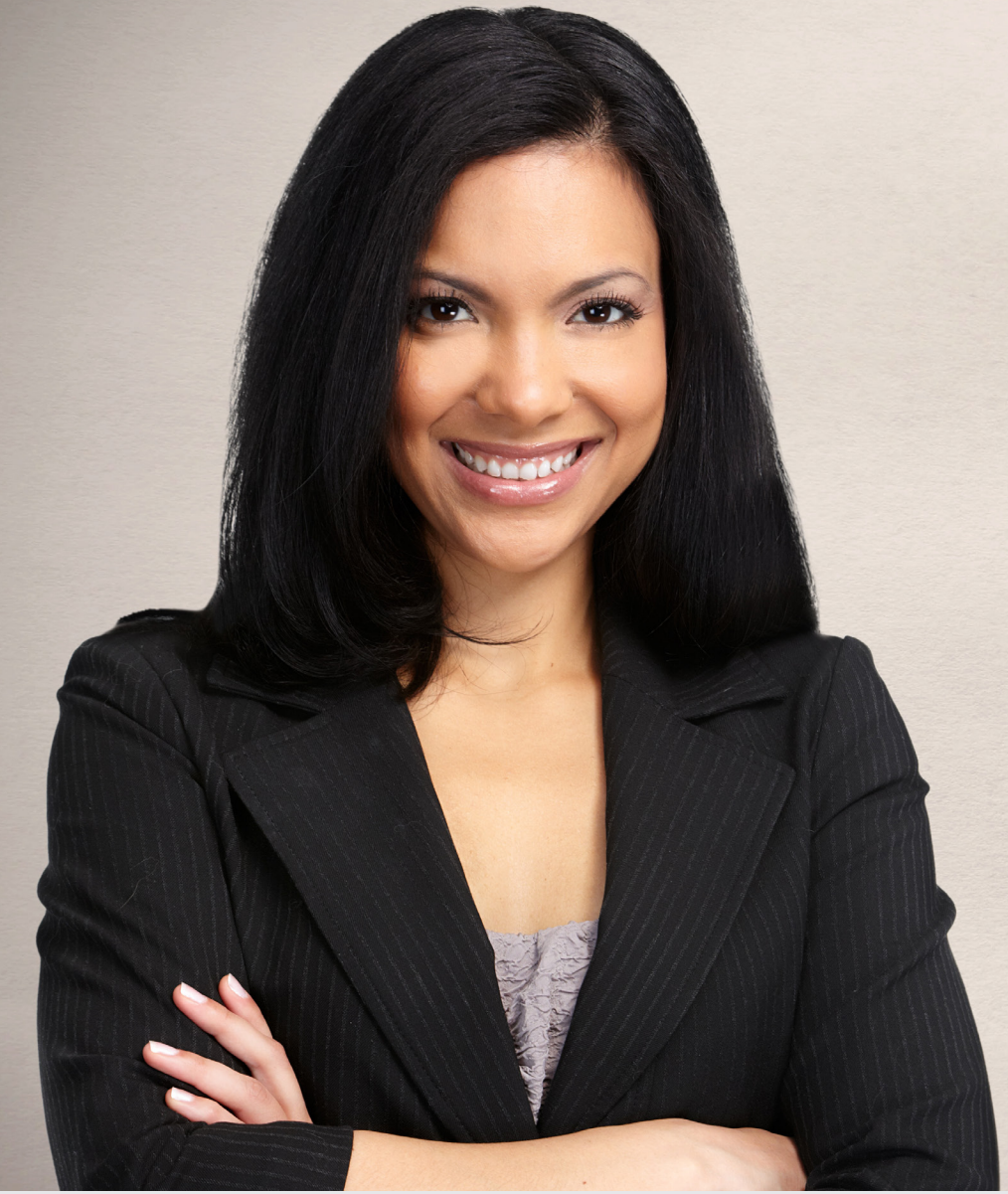
Élément humain (erreur humaine)

Exemple de scénario

L'un des employés de votre entreprise clique accidentellement sur un lien malveillant dans un courriel professionnel, ce qui provoque l'infection de votre ordinateur et de vos systèmes par un virus, rendant ainsi votre ordinateur inutilisable (exemple similaire mentionné précédemment dans la section, Coûts d'extorsion et perte d'exploitation). « L'élément humain » est l'une des causes les plus courantes d'atteinte cybernétique. Une formation inappropriée, des employés malhonnêtes et la négligence peuvent tous mener à une erreur humaine, ce qui peut entraîner des réclamations coûteuses et des pertes financières pour vous et votre entreprise.

Conseil

Une formation et une sensibilisation continues sont essentielles pour éviter les erreurs humaines. Assurez-vous que votre entreprise a mis en place des protocoles de sécurité et de protection des renseignements personnels et que vos employés en ont connaissance. Testez régulièrement vos employés pour évaluer ces connaissances. Vérifiez les vulnérabilités. Envisagez une approche proactive lorsque vous vous protégez, ainsi que vos employés et votre entreprise, contre les cyberattaques.



Comme vous pouvez le constater, ce ne sont là que quelques-uns des risques liés à la cyber-responsabilité auxquels vous pourriez être exposés en raison des technologies, des processus et des personnes que vous avez mis en place pour gérer votre entreprise.
Que vous possédiez ou gériez une entreprise, assurez-vous d'avoir une couverture liée à la cyber-responsabilité pour vous protéger, vous et votre entreprise, des cyberattaques.

#LaMenaceEstRéelle

Pour plus d'informations, visitez assurancevictor.ca ou consultez les ressources supplémentaires suivantes :

- Assurance contre les cyber-risques de Victor (auparavant ENCON)
- Ressources sur la COVID-19
- Infographie : « Journée typique dans la vie d'un propriétaire d'entreprise »
- Infographie : « Les cyberattaques : Une menace pour toutes les entreprises »
- Guide : « Cybersécurité : Travailler en toute sécurité depuis son domicile »
- Vidéo animée : « Une journée dans la vie d'un propriétaire d'entreprise dans un cybermonde »
- Vidéo : « Les experts de Victor partagent les mesures préventives alors que les cyberattaques se multiplient »

Visitez assurancevictor.ca pour en apprendre davantage.