lavery Avocats
QUOI FAIRE EN CAS DE CYBERINCIDENT AVANT PENDANT APRÈS VOS OBLIGATIONS QUESTIONNAIRE TECHNOJURIDIQUE
Des exemples de mesures de sécurité à instaurer | L'élaboration d'un plan de gestion | Avez-vous un plan de communication en cas de cyberincident? | Avez-vous une politique de confidentialité? | La sensibilisation des employés | Pourquoi l'assurance contre les cyberrisques

QUOI FAIRE AVANT

1

Impliquer vos administrateurs et vos directeurs

Avoir un conseil d'administration et une équipe de direction informés et actifs en cybersécurité est la clé. Voici quelques mesures qui peuvent vous guider dans cette tâche :

- Inclure la technologie dans les compétences du CA
- Créer une stratégie impliquant le CA et les dirigeants assurant la respect des obligations en cybersécurité
- Créer un système d'information efficace

2

Votre équipe d'intervention

Créez une équipe d'intervention qui pourra réagir dès le signalement d'un incident. Elle devra évaluer la gravité de l'incident et le documenter afin de tenter d'éviter un nouvel incident.

Cette équipe contient généralement les membres des départements :
TI
Ressources humaines
Gestion
Juridique
Communication

3

Mise en place de mesures de sécurité

Les lois prévoient que vous devez mettre en place des mesures de sécurité pour assurer la confidentialité des renseignements personnels qui vous ont été communiqués.

Ceci doit se faire, entre autres, par la mise en œuvre de moyens administratifs (Ex. mise en place de politiques), matériels et techniques.

DES EXEMPLES DE MESURES DE SÉCURITÉ À INSTAURER

Que vous ayez en votre possession des renseignements personnels ou des secrets commerciaux, vous devez en assurer la protection. Mettre en place ces mesures est aussi important pour éviter d'engager votre responsabilité en cas de litige.

- Configuration de tous les logiciels au plus haut paramètre de sécurité
- Authentification à double facteur
- Mise en place de logiciels de sécurité de type antivirus et d'audit interne automatisé
- Sécurisation des services mobiles
- Sauvegarde chiffrée des renseignements importants
- Application systématique des rustines (patches) de sécurité des logiciels, systèmes d'exploitation et tout le matériel technologique utilisé

NOTRE QUESTIONNAIRE TECHNOJURIDIQUE EST DISPONIBLE POUR VOUS AIDER

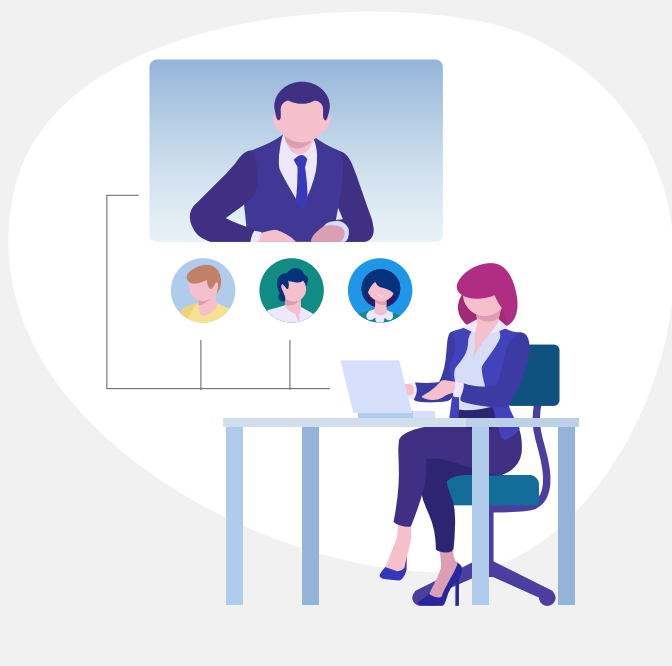
REMPLIR LE QUESTIONNAIRE

PLANIFIER ET PRÉVENIR UN CYBERINCIDENT

L'élaboration d'un plan de gestion

À quoi sert un plan de gestion:

- Permet à l'organisation de réagir rapidement et efficacement pendant un cyberincident.
- Permet de gérer en situation de crise la protection des renseignements personnels et des secrets commerciaux.
- Limite les dommages pouvant être causés par le cyberincident.



La communication du plan

Une fois votre plan créé, il doit être communiqué à votre conseil d'administration, vos dirigeants et tous vos employés selon leur niveau d'implication. Pour vous assurer que toutes les personnes concernées comprennent le fonctionnement du plan, pensez à effectuer une formation sur sa mise en œuvre.

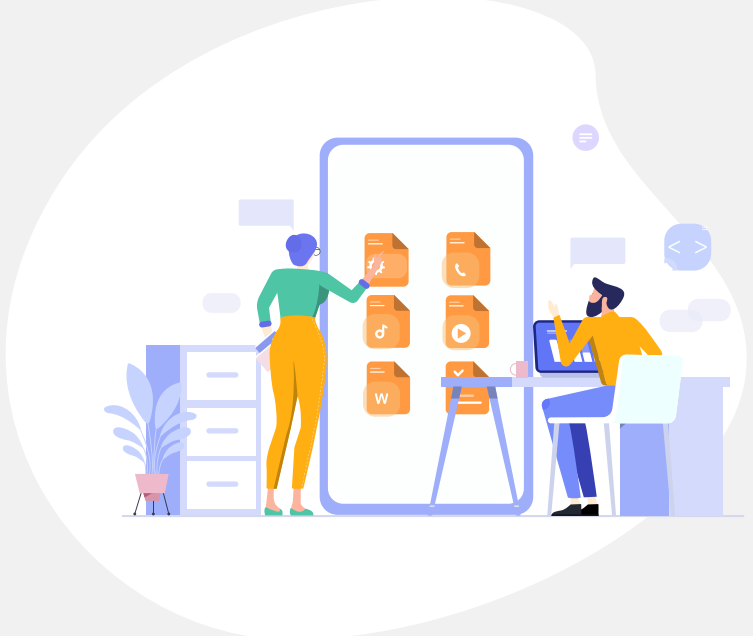
QUE DOIT CONTENIR VOTRE PLAN DE GESTION?

- Les objectifs et les procédures connexes
- Le champ d'application du plan
- Les rôles et les responsabilités de l'équipe d'intervention
- Les mesures à prendre par rapport au signalement de l'incident
- La catégorisation de la gravité des incidents
- Les étapes d'intervention lors de l'incident
- La procédure de vérification/audit
- La procédure de mise à jour du plan

La mise en oeuvre du plan

Effectuez des simulations de cyberincidents pour tester l'efficacité de votre plan. Assurez-vous de mettre à jour et de tester votre plan au moins annuellement et à la suite de tout cyberincident.

Le plan doit également être révisé régulièrement en fonction du roulement du personnel et de l'évolution des tâches de chacun.



AVEZ-VOUS UN PLAN DE COMMUNICATION EN CAS DE CYBERINCIDENT ?

Que vous ayez en votre possession des renseignements personnels ou des secrets commerciaux, vous devez en assurer la protection. Mettre en place ces mesures est aussi important pour éviter d'engager votre responsabilité en cas de litige.

Les questions clés

Votre plan de communication doit répondre aux questions suivantes:

1. **À qui communiquer?**
2. **Quoi communiquer?**
3. **Comment communiquer?**

Communication à l'interne

Votre plan devra indiquer comment un cyberincident sera signalé et comment vous transmettrez des informations à votre CA, à vos dirigeants et à vos employés.

Alternatives

Prévoyez vos modes alternatifs de communication tant à l'interne qu'à l'externe.

Par exemple, vous pouvez faire affaire avec une entreprise de service d'appel conférence ou créer des adresses courriel secondaires.

Communication à l'externe

Prévoyez votre mode de communication à l'externe avec les autorités, vos clients et vos partenaires d'affaires.

Créez des gabarits de notification de cyberincident pour être plus efficace.

Créez un tableau vous permettant d'identifier rapidement les informations de contact des clients et tiers qui ont des relations avec votre entreprise.

Les responsables

Précisez dans votre plan qui sont les personnes responsables de la communication à l'interne et à l'externe.

AVEZ-VOUS UNE POLITIQUE DE CONFIDENTIALITÉ ?

Votre politique de confidentialité doit prendre en compte les enjeux liés à la cybersécurité. Elle vous permettra de gérer l'accès et l'utilisation des renseignements personnels détenus par votre organisation et de vos secrets commerciaux.

Elle doit informer les employés sur la gestion des renseignements personnels et des secrets auxquels ils ont accès.

Elle est considérée par les entreprises comme l'un des moyens les plus efficaces pour contrer une utilisation non autorisée de secrets commerciaux.

NOTRE CABINET

Lavery peut vous aider à bâtir une politique de confidentialité efficace et vous conseiller quant à la mise en œuvre de votre politique de communication.

CE QUE VOTRE POLITIQUE DEVRAIT PRÉVOIR

- Les catégories de données pour y attribuer le niveau de protection nécessaire
- La gestion des informations confidentielles et personnelles par le personnel
- Des limites d'accès aux informations sensibles

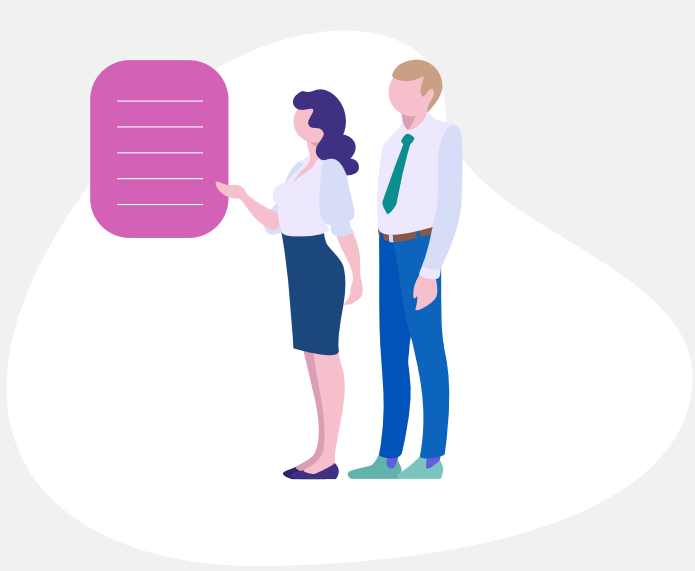
LA SENSIBILISATION DES EMPLOYÉS

La sensibilisation est une obligation, mais c'est aussi une étape cruciale de la prévention. Plusieurs incidents de cybersécurité sont causés involontairement par les employés.

1

L'importance de la cybersécurité

Vos employés doivent savoir comment la cybersécurité s'inscrit dans la culture de votre entreprise.



2

Confort avec les politiques de l'entreprise

Vos employés doivent:

- Être confortables avec l'application du plan de gestion d'incident
- Savoir quelles mesures de sécurités leur sont applicables
- Appliquer correctement le plan de communication et la politique de confidentialité de l'entreprise

Pour tester leurs réactions, pensez à procéder à des démarches d'ingénierie sociale (Ex. tests d'hameçonnage).

3

Utilisation du matériel informatique

Pensez à créer une politique sur l'utilisation du matériel informatique pour que votre personnel sache quelles sont les précautions à prendre (Ex. Ne pas laisser son ordinateur de bureau sans surveillance dans un endroit public).

4

Utilisation du matériel informatique personnel

Si vous permettez à vos employés d'utiliser leur ordinateur portable ou téléphone personnel, vous aurez moins de contrôle sur les mesures de sécurité.

Vous pouvez tout de même mettre à la disposition de vos employés:

- Une liste d'applications testées
- Des mesures de sécurité recommandées
- Recommander des tests diagnostic sur leur ordinateur

ASSURANCE CYBERRISQUES

Pourquoi l'assurance contre les cyberrisques

1

Les politiques d'assurance générales excluent souvent les pertes qui peuvent résulter d'un cyberincident.

2

Les assurances cyberrisques peuvent couvrir plusieurs des pertes encourues lors d'un cyberincident et assurer la défense en cas de poursuites.

Dépenses pouvant être encourues en raison d'un cyberincident :

- Frais de notification
- Pertes financières liées à l'interruption de vos services
- Frais d'analyse du cyberincident par des experts
- Frais liés à la gestion d'une crise

Dépenses reliées aux poursuites judiciaires :

- Les dommages à payer en cas d'accès non autorisé à des renseignements personnels ou confidentiels pourraient être couverts
- Les frais juridiques

LA CYBERSÉCURITÉ…

QUOI FAIRE AVANT
- Prévenir un cyberincident
- Planifier une réponse

QUOI FAIRE PENDANT
- Détection et signalement
- Confinement de l'incident et enquête

QUOI FAIRE APRÈS
- Votre obligation de divulgation
- Préservation des traces de l'incident
- Améliorations à vos processus

MONTRÉAL
Bureau 4000
1, Place Ville Marie
Montréal QC H3B 4M4
Itinéraire
Téléphone : 514 871-1522
Télécopieur : 514 871-8977

QUÉBEC
Bureau 500
925, Grande Allée Ouest
Québec QC G1S 1C1
Itinéraire
Téléphone : 418 688-5000
Télécopieur : 418 688-3458

SHERBROOKE
Bureau 200, Cité du Parc
95, Boul. Jacques-Cartier Sud
Sherbrooke QC J1J 2Z3
Itinéraire
Téléphone : 819 346-5058
Télécopieur : 819 346-5007

TROIS-RIVIÈRES
Bureau 360
1500, rue Royale
Trois-Rivières QC G9A 6E6
Itinéraire
Téléphone : 819 373-7000
Télécopieur : 819 373-0943

© 2021 Lavery de Billy, S.E.N.C.R.L. Tous droits réservés.