CLASSESAFFAIRES
ACTUALITÉS ▪ SÉMINAIRES ▪ PERSPECTIVES

Blakes

Liste de vérification pour réduire les risques

PERSONNE-RESSOURCE
Hélène Deschamps Marquis
Associée
hdm@blakes.com
514-982-4042

Avant l'incident

- ☑ Élaborer une structure officielle de gouvernance de l'information
- ☑ Mettre sur pied une équipe pour la sécurité de l'information à l'échelle de l'entreprise
- ☑ Préparer un diagramme de flux de données et faire une analyse des risques relatifs aux données
- ☑ Mettre en place un plan d'intervention en cas d'incident
- ☑ Offrir des formations de sensibilisation à la protection de la vie privée et à la sécurité
- ☑ Élaborer un programme de gestion des fournisseurs
- ☑ Réaliser un exercice d'intervention en cas d'incident
- ☑ Évaluer l'assurance contre les cyberrisques

Après l'incident

- ☑ Agir rapidement
- ☑ Suivre le plan d'intervention en cas d'incident
- ☑ Embaucher des experts
- ☑ Faire une enquête sur l'incident et en limiter les répercussions
- ☑ Protéger le secret professionnel
- ☑ Tenir compte des exigences de notification
- ☑ S'assurer que la stratégie de communication minimise les risques de litige
- ☑ Gérer les communications avec les employés

CLASSESAFFAIRES
ACTUALITÉS ▪ SÉMINAIRES ▪ PERSPECTIVES

Blakes

Plan d'intervention en cas d'incident – Liste de vérification

PERSONNE-RESSOURCE
Hélène Deschamps Marquis
Associée
hdm@blakes.com
514-982-4042

Toute entreprise devrait avoir un plan expliquant comment réagir à une cyberattaque potentielle. Pour être utile en cas d'incident, le plan ne devrait être ni trop long ni trop court. Voici une liste de vérification à suivre sur la façon de créer un plan d'intervention efficace en cas d'incident :

1re étape : Élaborer le plan

- ☑ Former une équipe d'intervention.
- ☑ De quelle façon communiquera-t-on avec l'équipe d'intervention?
- ☑ Qui contactera l'assureur (contrat d'assurance cyberrisques)?
- ☑ Qui aviser et quand (conseil d'administration, clients, autorités de réglementation, organismes d'application de la loi, etc.)?
- ☑ Établir des mesures d'intervention technologique spécialisées comme l'embauche de tiers au besoin.
- ☑ Comment documenter les mesures prises?
- ☑ Comment protéger le secret professionnel au cours de l'enquête?
- ☑ Nommer un porte-parole au sein de l'équipe qui s'adressera aux médias.
- ☑ Comment réduire le risque de litige?
- ☑ Quels sont les enjeux à l'échelle mondiale (p. ex. différentes lois/pratiques relatives aux renseignements personnels et à la protection de la vie privée)?

2e étape : Mettre le plan à l'épreuve

- ☑ Procéder à une simulation, évaluer l'intervention de votre société et ajuster le plan en conséquence.
- ☑ Documenter les résultats de la simulation afin de prouver que vous prenez la cybersécurité au sérieux.
- ☑ Fournir aux membres des équipes interfonctionnelles (conseillers juridiques, TI et hauts dirigeants) des occasions de se connaître et d'en savoir davantage sur l'expertise de chacun en cybersécurité.
- ☑ Nommer des leaders chargés de mettre en œuvre le plan (le chef des TI pour l'intervention technologique, le conseiller juridique pour la communication avec le conseil d'administration et les hauts dirigeants, etc.).

3e étape : Embaucher des tiers

- ☑ Conclure au préalable des ententes avec des fournisseurs (conseiller en relations publiques, analyste judiciaire, conseiller juridique externe, etc.).

4e étape : Tenir le plan à jour

- ☑ Mettre le plan à jour périodiquement. Il ne sera d'aucune utilité si, par exemple, il y est indiqué qu'il faut communiquer avec le chef des TI alors que celui-ci ne travaille plus pour la société.