Baker McKenzie.

Tips & Tricks
Cybersécurité

Cybersécurité: quelle responsabilité personnelle pour le dirigeant en cas d'attaque?

Victime d'un ransomware, une entreprise voit soudainement son activité paralysée et certaines de ses données les plus sensibles divulguées sur le darkweb. Le préjudice est considérable. Focus sur la responsabilité personnelle du dirigeant.

PLUSIEURS FONDEMENTS POUR ENGAGER LA RESPONSABILITÉ PERSONNELLE DU DIRIGEANT

Responsabilité personnelle civile et/ou pénale du dirigeant : jusqu'à **5 ans** d'emprisonnement et **300.000 EUR** d'amende en matière pénale.

Peuvent être reprochés au **dirigeant**:

- négligence et insuffisance de préparation de l'entreprise
- manquement à l'obligation d'assurer la sécurité des données
- défaut de notification de la violation de données aux autorités de contrôle et aux personnes concernées

PLUSIEURS ACTEURS PEUVENT AGIR CONTRE LE DIRIGEANT

Plusieurs acteurs ont vocation à venir demander des comptes au dirigeant pour le préjudice subi par l'entreprise ou pour leur préjudice personnel, s'il a commis des fautes :

Les actionnaires
- pour le préjudice subi par **l'entreprise:** action pour le compte de la société (***ut singuli/ut plures***)
- pour leur préjudice individuel, à charge de démontrer un préjudice personnel, distinct de celui de la société

Les autres dirigeants (ou les nouveaux dirigeants)
- action au nom de la société (***ut universi***)

Les autorités de contrôle et le Ministère public
- Plainte pénale

POUR EVITER DE VOIR SA RESPONSABILITE ENGAGEE, LE DIRIGEANT DOIT INTÉGRER LES RISQUES LIÉS A LA CYBERSÉCURITÉ ET DOUBLEMENT SE PRÉPARER

Se protéger personnellement…

1) Mettre en place des **délégations de pouvoirs** et de **responsabilité pénale**
   - vérifier la **compétence** et l'autorité effective du délégataire,
   - rédiger une délégation **expresse**, **précise** et **limitée,**
   - donner au délégataire **les moyens nécessaires** pour accomplir sa mission.

2) Souscrire une **assurance** à titre personnel couvrant les **risques de cybersécurité**

3) Inscrire le **risque cyber** au plus haut niveau des préoccupations de l'entreprise et le mettre à **l'agenda du Comex / Conseil d'Administration**

… et protéger son entreprise

1) Mettre en place une **gouvernance** adaptée et s'entourer des bonnes personnes (fonctions et comités)

2) Mettre en place les **procédures et politiques** nécessaires pour gérer la cybersécurité, les documenter et les intégrer dans la gouvernance

3) Intégrer la **gestion du risque cyber** dans le quotidien de l'entreprise
   - investir dans des outils performants de détection et de correction d'attaques
   - former le personnel
   - simuler des crises et tester systématiquement

Notre équipe est N°1 en **IT & Internet et protection des données** - *Chambers Global & Legal 500 2020* : elle vous accompagne en matière contractuelle, réglementaire et contentieuse, dans vos projets innovants, complexes et souvent internationaux, la transformation digitale, la communication électronique, les données personnelles et la cybersécurité. Nous contacter : paritc@bakermckenzie.com

www.bakermckenzie.com