

# SÉCURITÉ : QUEL EST LE RÔLE D'UN AVOCAT ?

Chez ITLAW Avocats, nous accompagnons depuis plusieurs années nos clients dans le cadre de la gestion de crise dite de nature "cyber".

Nous observons ainsi que le sujet (cyber)sécurité présente les principales caractéristiques des crises dites « majeures » que peut traverser une entreprise à savoir un impact majeur pour l'entreprise, pouvant être temporaire et/ou futur : arrêt de fonctionnement, perte de chiffres d'affaires, perte de données, perte d'image auprès de tiers notamment les clients, etc..

## EXISTE-T-IL DES SPÉCIFICITÉS LIÉES À UNE CRISE (CYBER)SÉCURITÉ ?

Oui, nous pouvons relever deux spécificités majeures :

### 1/ Un impact et une complexité technique d'ampleur :

Nous observons que cette particularité cyber a pour effet que bien souvent l'entreprise ne dispose pas des ressources nécessaires en interne soit parce que cela nécessite une expertise très qualifiée et/ou rare soit parce que la quantité de ressources est insuffisante (les ressources devront à la fois se mobiliser sur la correction du problème cyber et pour que l'entreprise puisse continuer à fonctionner).

Bien évidemment, les entreprises ayant anticipé ce risque sont plus résilientes face aux crises cyber.

Comment l'anticiper ? Nous proposons deux axes :

- Prévoir dans ses contrats avec ses fournisseurs IT notamment les modalités de leur coopération ainsi que les conditions financières, et ;
- Prévoir par anticipation quel tiers (prestataire IT, avocat, huissier, etc...) pourra vous accompagner et selon quelles modalités.

### 2/ Une maîtrise incontournable des enjeux juridiques :

Nous constatons que malheureusement peu d'entreprises prennent conscience des enjeux juridiques qui d'ailleurs ne figurent pas dans les PRA et/ou PCA ni dans les procédures de gestion d'incident de sécurité.

## QUELS SONT LES ENJEUX JURIDIQUES QU'IL EST NÉCESSAIRE D'APPRÉHENDER ?

La particularité des risques en matière de (cyber)sécurité réside dans la combinaison de plusieurs responsabilités : pénale, administrative, contractuelle, civile ...

Ainsi, le premier enjeu juridique est de taille, il s'agit de réagir de manière conforme à la loi. En effet, il existe des obligations légales à respecter lors d'un incident de sécurité, sous peine d'engager sa responsabilité. Attention, ces obligations sont disparates dans les textes de loi.

Elles peuvent concerner un secteur, le statut de l'entreprise et la nature de l'incident (ex : violation de données à caractère personnel). Le second concerne le respect de ses obligations vis-à-vis des tiers, notamment les obligations contractuelles. Il est impératif de respecter ces dispositions sous peine de voir la responsabilité de l'entreprise engagée par ses cocontractants.

Enfin le dernier enjeu sur lequel nous attirons l'attention concerne la préservation des intérêts de l'entreprise. À savoir identifier, préserver et conserver de manière adéquate les éléments de preuve de l'incident, saisir les autorités publiques, avertir son assureur.

## ARTICLE RÉDIGÉ PAR



**CLAUDIA WEBER**

Avocat fondateur  
cabinet ITLAW Avocats



**MARINE HARDY**

Avocat directeur des  
pôles Innovation &  
Sécurité ITLAW Avocats

## Comment ITLAW accompagne les entreprises ?

La crise (cyber)sécurité est une épreuve humaine pour les équipes de l'entreprise impactée et les risques de responsabilités sont forts et nombreux.

Aussi chez ITLAW Avocats, nous prenons en main les enjeux juridiques pour limiter les risques, notamment en matière de responsabilité et permettre à nos clients de se concentrer sur les travaux techniques et la gestion de la crise.

### Une question ?

[contact@itlaw.fr](mailto:contact@itlaw.fr)

01.83.62.61.75