Les Petites Affiches de Vaucluse depuis 1839

Ecrit par Echo du Mardi le 6 juillet 2026

Cyberattaque : et si votre avocat était votre premier rempart juridique ?

En France, 60 % des PME victimes de cyberattaque n'ont pas d'avocat dans leur cellule de crise, ce qui a pour résultat des plaintes mal rédigées, assurances non indemnisées, responsabilités mal gérées. Maitre Djamel Belhaouci* du barreau de Marseille explique pourquoi l'avocat est un acteur incontournable dès la première heure.

Il est 2h du matin, les serveurs d'une PME francilienne viennent d'être chiffrés par un ransomware. Le dirigeant réveille son DSI, contacte son prestataire informatique, alerte son assureur. L'avocat ? Il sera appelé trois semaines plus tard, hélas quand il sera trop tard pour réparer la plupart des erreurs commises.

> « Une entreprise victime de cyberattaque a 72 heures pour notifier la CNIL d'une éventuelle fuite de données. »

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par Echo du Mardi le 6 juillet 2026

Maître Djamel Belhaouci

Ce scénario, Maître Belhaouci, avocat en droit de la cybercriminalité, le rencontre chaque semaine dans son cabinet. « Les entreprises pensent que la cyberattaque est d'abord un problème technique. C'est une erreur fondamentale, dès la première heure, elle est surtout un problème juridique. »

« Une entreprise victime de cyberattaque a 72 heures pour notifier la CNIL d'une éventuelle fuite de données. Si cette notification est absente, mal rédigée ou tardive, les sanctions peuvent dépasser le préjudice de l'attaque elle-même. Il est de même pour le dépôt de plainte dans le cadre d'une couverture assurantielle. C'est le premier acte juridique à poser et il doit l'être par un avocat. »

Rappel du cadre légal
Notification CNIL obligatoire : 72 heures après la découverte d'une violation de données à caractère personnel (art. 33 RGPD). Information des personnes concernées : sans délai injustifié lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés (art. 34 RGPD). Infractions applicables : accès frauduleux à un STAD (art. 323-1 CP), atteinte au secret des affaires (loi du 30 juillet 2018), extorsion (art. 312-1 CP).
Face à la recrudescence des cyberattaques en France le nombre d'incidents déclarés à l'ANSSI a progressé de 30% en 2025 , Maitre Belhaouci appelle les chefs d'entreprise à anticiper : « Intégrez votre avocat dans votre plan de continuité d'activité avant la crise. Le moment le plus coûteux pour appeler un avocat spécialisé, c'est le lendemain de l'attaque. »

Les trois erreurs récurrentes commises en l'absence d'un avocat
1. La plainte rédigée sans conseiller juridique: dans la précipitation, les dirigeants déposent des plaintes incomplètes, sans qualification précise des infractions tel l'accès frauduleux à un système de traitement automatisé de données (STAD), l'extorsion, l'atteinte au secret des affaires. Une plainte mal rédigée affaiblit l'ensemble de la procédure pénale et réduit les chances d'indemnisation.

2. L'assureur cyber contacté sans préparation: les polices d'assurance cyber contiennent des clauses d'exclusion précises. Contacter l'assureur sans avoir préalablement sécurisé les preuves et documenté l'incident avec un conseil juridique expose l'entreprise à un refus de garantie. « J'ai vu des entreprises perdre plusieurs centaines de milliers d'euros d'indemnisation pour des déclarations maladroites faites dans les premières heures », témoigne Maitre Belhaouci.

3. La communication de crise sans garde-fou juridique: informer ses clients, ses partenaires ou la presse d'une violation de données engage la responsabilité civile et pénale de l'entreprise. Chaque mot compte. L'avocat est le seul interlocuteur capable de valider ces communications sous couvert du secret professionnel.

« Ce n'est pas une question de taille d'entreprise. »

Ecrit par Echo du Mardi le 6 juillet 2026

L’avocat dans la cellule de crise : un investissement, pas un coût Maître Belhaouci plaide pour une intégration systématique de l’avocat spécialisé en cybercriminalité dans les plans de réponse aux incidents des entreprises au même titre que le responsable informatique ou le DPO. « Ce n’est pas une question de taille d’entreprise. Une PME de 20 salariés est aussi concernée qu’un groupe du CAC 40. Les cyberattaquants ne font pas de distinction. »

Concrètement, l’intervention de l’avocat dès la première heure permet : la préservation des preuves dans des conditions juridiquement recevables, la rédaction de la notification CNIL dans les délais légaux (72 heures), le pilotage de la relation avec les forces de l’ordre et le parquet cybercriminalité, la sécurisation des communications internes et externes, et l’anticipation des recours des tiers éventuellement affectés.

L.G.

**Maître Djamel Belhaouci est avocat au Barreau de Marseille. Il dirige un cabinet dédié au droit de la cybercriminalité et en défense pénale. Il intervient dans les procédures pénales liées aux infractions informatiques, conseille les entreprises victimes de cyberattaques et accompagne ses clients dans leur mise en conformité.*