

Checklist – événement Cyber - HISCOX

En cas d'attaque cyber ou de suspicion, les mesures d'urgence à prendre sont les suivantes :

- 1. Contacter immédiatement l'assistance de votre assureur, disponible (24/7) au +33 (0)1 78 41 58 12**
- 2. Déposer plainte, en respect de la LOPMI, dans un délai de 72 heures à compter de la découverte de l'incident. A défaut, l'assureur ne pourra pas appliquer les garanties du contrat**

Vous pouvez déposer plainte :

- A la gendarmerie ou au commissariat de votre choix : se faire remettre le procès-verbal de dépôt de plainte afin d'en conserver une preuve écrite ;
- Par courrier en Recommandé avec Accusé Réception adressé au Procureur de la République près le Tribunal judiciaire du lieu des faits ou du domicile de l'auteur des faits s'il est connu

ATTENTION : La pré-plainte en ligne n'est pas suffisante pour le respect des obligations légales

En cas d'attaque ou de suspicion d'attaque **subie à l'étranger** (une entreprise française, assurée par un contrat soumis au droit français et victime d'une cyberattaque à l'étranger) : il convient de déposer plainte en France ET dans le pays où la cyberattaque a eu lieu. **Le délai de 72 heures doit être respecté.**

- 3. Déclarer le sinistre à AON : declaration.cyber@aon.com**

- 4. Notifier toute autorité administrative compétente dans le délai de 72 heures**

La CNIL, en cas d'atteinte aux données personnelles, l'ANSSI...

- 5. Activer le plan de continuité des activités (PCA) et de reprise après sinistre**

Il est essentiel d'activer votre PCA et éventuellement solliciter votre équipe interne de réponse à incident cyber, la direction juridique, le service contentieux...

- 6. Comment réagir face à un Ransomware / une demande d'extorsion ?**

Ne pas initier de réponse à l'attaquant sans avoir échangé avec votre assureur et/ou un professionnel de la négociation. Votre assureur pourra vous recommander un professionnel chargé de négocier avec les attaquants en votre nom.

- 7. Informer le délégué à la protection des données (DPO)**

Les responsables du traitement des données/contrôleurs des données ont des obligations strictes en vertu du RGPD et d'autres réglementations similaires en dehors de l'UE, notamment dans le cas où une notification serait nécessaire.

- 8. Traiter les communications internes et externes**

Faire appel à des conseillers en gouvernance et en communication de crise pour vous épauler dans la stratégie de communication interne / externe. Les assureurs disposent d'un panel de prestataires si besoin.