

## RÉFLEXES CYBER

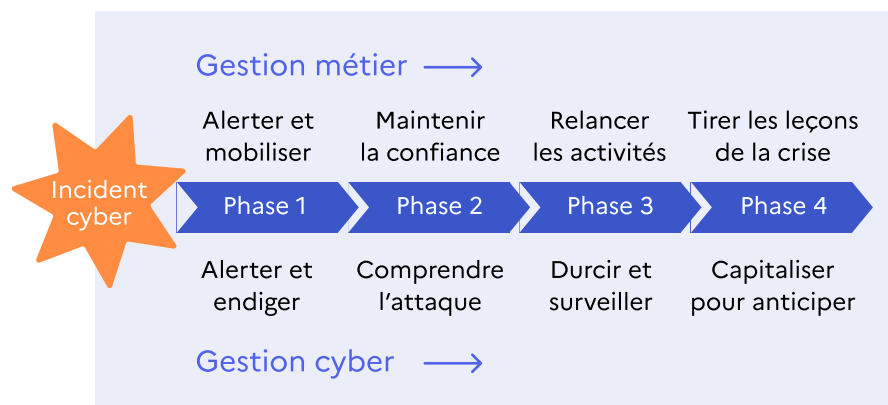
## MES PREMIERS RÉFLEXES EN CAS D'INCIDENT CYBER

## RÉFLÈXES CYBER

# Les grandes étapes d'une gestion de crise cyber

Généralement, les actions des équipes s'articulent autour de quatre grandes phases de crise :

- Alerter, mobiliser le personnel et arrêter la propagation de l'attaque pour protéger les bénéficiaires et l'organisation
- Comprendre le schéma d'attaque, éjecter l'attaquant, déployer des mesures pour potentiellement travailler sans services et sans outils numériques et communiquer auprès de son écosystème pour maintenir la confiance
- Durcir les systèmes, restaurer les applications et les données critiques et surveiller l'attaquant pour reprendre le cœur des activités
- Revenir à la normale et organiser un retour d'expérience



## RÉFLÈXES CYBER

# Mes réflexes d'urgence

En cas de comportement suspect sur les ordinateurs (ex : écran noir, message revendiquant une cyberattaque), j'alerte les équipes en charge de l'informatique.

En fonction des consignes passées, je peux aider à débrancher l'ensemble des machines (ordinateurs ou serveurs du réseau) sans les éteindre / je n'allume pas les machines éteintes.

## RÉFLÈXES CYBER

# **Vous êtes responsable informatique**

Vous êtes chargé(e) de conseiller la direction sur les choix techniques et technologiques, y compris les enjeux de cybersécurité.

Vous pilotez la mise en œuvre des décisions stratégiques liées à l'informatique et veillez à l'alignement des systèmes avec les objectifs de l'entreprise.

Vous supervisez les équipes informatiques, gérez les projets de transformation numérique.



## **Quelques risques en cas de crise d'origine cyber :**

- Blocage ou compromission des systèmes.
- Exfiltration de données
- Surcharge et pression opérationnelle.

# **Agir en tant que responsable informatique**

## **En cas de crise cyber :**

- Je demande aux équipes ou à l'infogérant d'investiguer sur les origines de l'incident afin d'identifier sa nature et ses impacts opérationnels.
- Je sollicite une aide extérieure pour la résolution technique de l'incident.
- Je mets en place des actions pour empêcher l'expansion de l'attaque (ex : isoler le réseau).
- Je vérifie si des serveurs de sauvegardes existent et s'ils sont bien isolés. Si ce n'est pas le cas, je les débranche du réseau.
- Je demande à la direction d'arbitrer l'action de couper (ou non) la connexion à Internet pour éviter la propagation de l'attaque (via la box ou le cœur de réseau). J'isole *a minima* la zone infectée.

## RÉFLÈXES CYBER

# **Vous êtes responsable de la communication**

Vous êtes responsable de la stratégie de promotion et de communication de l'organisation. Vous supervisez les campagnes de communication internes et externes, et veillez à l'image de l'organisation.

Vous travaillez en étroite collaboration avec les autres départements pour aligner les messages et les actions sur les objectifs stratégiques.



## **Quelques risques en cas de crise d'origine cyber :**

- Atteinte à l'image et à la réputation.
- Désinformation et perte de maîtrise du discours.
- Pression accrue dans la gestion de crise.

# **Agir en tant que responsable de la communication**

## **En cas de crise cyber :**

- J'identifie les moyens à ma disposition pour communiquer efficacement (interne/externe).
- J'établis un plan de communication en lien avec les équipes métiers et informatique, et en fonction des publics ciblés (publics, supports, moyens de diffusion, contenu des messages, temporalité).
- J'exige que l'ensemble des demandes de communication soient transmises au service communication.
- Je nomme un porte-parole pour répondre aux médias.
- Si la crise n'est pas encore médiatisée, je prépare des éléments de communication proactifs.



## **Vous êtes responsable des ressources humaines**

Vous coordonnez, gérez et contrôlez l'ensemble des procédures de gestion administrative des employés de l'entreprise, des agents ou collaborateurs de l'organisation (recrutement, paie, temps de travail).

Vous êtes très vigilant aux conditions de travail et aux risques psychosociaux.



### **Quelques risques en cas de crise d'origine cyber :**

- Tensions et conflits au sein de l'organisation.
- Risques psychosociaux pour les salariés.
- Atteinte à l'image de l'organisation.

## **Agir en tant que responsable des ressources humaines**

### **En cas de crise cyber :**

- J'informe, avec l'aide des autres responsables, les collaborateurs sur les consignes à tenir et l'évolution de la situation.
- Je m'assure que les agents ou les collaborateurs pourront être payés et cherche à organiser ce point en cas de dégradation du service.
- J'organise le travail des équipes pour répondre aux besoins de la crise (ex : horaires étendus, repos, mise au chômage partielle) et m'assure du respect des règles applicables à ces modes de travail exceptionnels.
- Je veille au bien-être physique et mental des employés de l'entreprise, des agents ou collaborateurs de l'organisation, et je les épaulé si nécessaire avec l'aide de professionnels (ex : psychologue).

## **Vous êtes responsable juridique**

Vous veillez à la conformité de l'organisation avec les lois et réglementations, supervisez les contrats et les contentieux, et conseillez la direction sur les décisions stratégiques.

Vous protégez les intérêts de l'organisation, gérez les risques juridiques et collaborez avec les autres départements, y compris en cas de crise ou de cyberattaque.



### **Quelques risques en cas de crise d'origine cyber :**

- Exposition à des sanctions légales et réglementaires.
- Hausse de la gestion des litiges et responsabilités.
- Perte de maîtrise de la communication légale.

## **Agir en tant que responsable juridique**

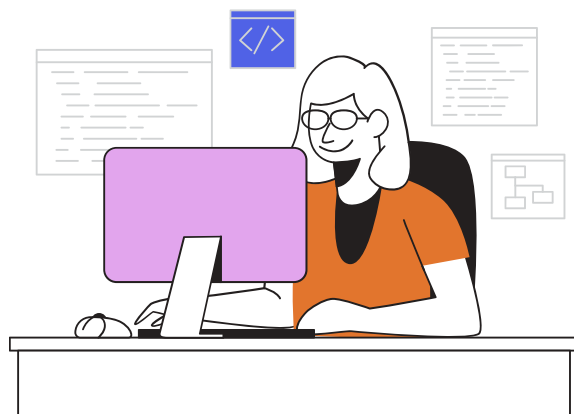
### **En cas de crise cyber :**

- J'identifie si certaines obligations auprès des clients ou administrés, des partenaires ou des fournisseurs ne peuvent pas être respectées et je propose une adaptation du plan de continuité d'activité.
- Je porte plainte auprès du commissariat de police ou de la brigade de gendarmerie dont l'organisation dépend (en parallèle de la résolution technique de l'incident), en s'appuyant sur le registre des événements et actions (main courante)
- Si une réglementation me l'impose, je signale mon incident à l'ANSSI et/ou à mes autorités de tutelle.
- En cas de fuite ou d'indisponibilité de données personnelles, je déclare l'incident auprès de la CNIL.
- Je n'hésite pas à solliciter mon assurance pour des actions de soutien (prestataires, prise en charge financière).

## **Vous êtes responsable relation usagers/clients**

Vous pilotez la mise en place de services vers les publics externes.

Vous proposez des solutions face aux problèmes rencontrés, en priorisant la satisfaction des usagers/clients.



### **Quelques risques en cas de crise d'origine cyber :**

- Perte d'accès des services dédiés aux usagers/clients
- Exposition de données personnelles ou professionnelles.
- Mécontentements et désorganisation.

## **Agir en tant que responsable relation usagers/clients**

### **En cas de crise cyber :**

- J'identifie les processus touchés (ex : applications externes, services) et propose une priorisation des actions de continuité / reprise des activités - en m'appuyant sur mon analyse et le contexte socio-économique.
- Je soutiens la réorganisation des activités, en fonction des priorités établies.
- Je relaye, avec l'aide de la communication, des informations sur l'indisponibilité des services aux usagers/clients.
- Je propose, si nécessaire, des compensations pour pallier un service dégradé.

## RÉFLÈXES CYBER

# **Vous êtes responsable financier**

Vous pilotez la préparation et l'analyse des états comptables et supervisez la trésorerie.

Vous cherchez à limiter les risques financiers et vous conseillez la direction sur ce volet.

Vous gérez la relation avec les parties prenantes externes (banques, investisseurs, partenaires économiques).



## **Quelques risques en cas de crise d'origine cyber :**

- Exposition à des poursuites ou sanctions judiciaires et financières.
- Retards de paiements.
- Risque de fraude interne/externe (ex : virements frauduleux, détournements).
- Risque de dépenses imprévues liée à la crise.

# **Agir en tant que responsable financier**

## **En cas de crise cyber :**

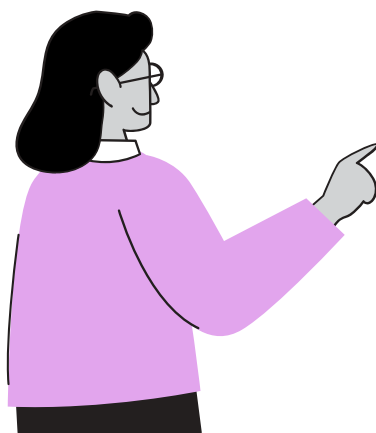
- J'identifie les processus financiers touchés (ex : paiements, trésorerie, facturation, salaires, etc) et propose une priorisation des actions de continuité/reprise des activités - en m'appuyant sur mon analyse et le contexte socio-économique.
- Je cherche à garantir la continuité de la trésorerie (ex : priorisation des paiements urgents - salaires, fournisseurs stratégiques, dettes fiscales/sociales - besoins en liquidités, surveillance des mouvements suspects).
- J'estime les coûts directs et indirect de l'attaque : (ex : perte de chiffre d'affaires, frais de restauration, turnover client, surcoûts opérationnels).
- Si une réglementation me l'impose, je déclare le sinistre (assurance, autorités).



## **Vous êtes responsable de l'organisation**

Vous pilotez la stratégie et la performance globale de l'organisation. Vous prenez les décisions clés pour garantir sa pérennité, son développement et sa réputation.

Votre rôle implique de coordonner les équipes, d'anticiper les risques et de maintenir la confiance des usagers, partenaires et collaborateurs.



### **Quelques risques en cas de crise d'origine cyber :**

- Impact financier et opérationnel majeur.
- Responsabilité juridique et stratégique de la direction.
- Atteinte à la crédibilité, la confiance et la réputation.

## **Agir en tant que responsable de l'organisation**

- Je rassemble une cellule de crise qui mobilise les décideurs métiers de l'organisation. L'ensemble des décisions relatives à la gestion de la situation sont validées par cette cellule, pilotée de préférence par la direction.
- La cellule de crise sera ensuite mobilisée selon un rythme défini par les besoins (ex : toutes les 2h au début de l'incident, tous les jours après quelques temps).
- J'organise des points de situations réguliers.
- Je tiens un registre des événements et actions réalisées (main courante) pour faciliter la conduite de la crise et pouvoir conserver une trace à disposition des enquêteurs et tirer les enseignements de l'incident *a posteriori*.
- Je liste, avec l'aide des responsables métiers, l'ensemble des services et activités impactés et travaille à la mise en place de solutions dégradées (plan de continuité d'activité) et / ou d'un plan de reprise des activités à l'arrêt.
- Je ne cherche pas de coupable auprès des équipes ou au niveau du prestataire.
- J'évite de payer une rançon en cas de demande.

RÉFLÈXES CYBER

## Mon prestataire informatique



Nom : \_\_\_\_\_

Prénom : \_\_\_\_\_

Téléphone : \_\_\_\_\_

Mail : \_\_\_\_\_

Notes :

RÉFLÈXES CYBER

## Ma banque



Nom : \_\_\_\_\_

Prénom : \_\_\_\_\_

Téléphone : \_\_\_\_\_

Mail : \_\_\_\_\_

Notes :

RÉFLÈXES CYBER

## Mon assurance



Nom : \_\_\_\_\_

Prénom : \_\_\_\_\_

Téléphone : \_\_\_\_\_

Mail : \_\_\_\_\_

Notes :

RÉFLÈXES CYBER

## Mes contacts utiles



Nom : \_\_\_\_\_

Prénom : \_\_\_\_\_

Téléphone : \_\_\_\_\_

Mail : \_\_\_\_\_

Notes :

RÉFLÈXES CYBER

## Mes contacts utiles



Nom : .....

Prénom : .....

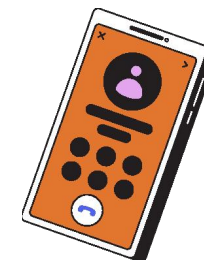
Téléphone : .....

Mail : .....

Notes :

RÉFLÈXES CYBER

## Mes contacts utiles



Nom : .....

Prénom : .....

Téléphone : .....

Mail : .....

Notes :