RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DE CRISE CYBER

ANTICIPER ET GÉRER SA COMMUNICATION DE CRISE CYBER

COLLECTION
GESTION DE CRISE CYBER

GUIDE

ANTICIPER ET GÉRER SA COMMUNICATION DE CRISE CYBER

Service du Premier ministre créé en 2009 et placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France. Le modèle français de la cybersécurité repose sur une séparation claire, au sein de l'État, entre les missions défensives et offensives, et l'ANSSI est chargée de coordonner le champ de la défense et de la protection des systèmes d'information.

La raison d'être de l'Agence est ainsi de construire et d'organiser, en interministériel, la protection de la Nation face aux cyberattaques et de contribuer à la stabilité du cyberespace. Son action s'inscrit dans le cadre des missions régaliennes de l'État, au service d'un objectif général de politique publique de sécurité et de résilience des administrations, de l'économie et de la société dans son ensemble.

L'ACTION DE L'ANSSI SE TRADUIT EN CINQ GRANDES MISSIONS

Défendre
les systèmes d'information
critiques et les victimes
de cyberattaques d'ampleur

Connaître
l'état de l'art de la cybersécurité
et les menaces du cyberespace

Partager
de la connaissance, des recommandations
et de l'expertise en sûreté numérique

Accompagner
l'écosystème national
et international

Réguler
les organisations, les produits
et les services de cybersécurité

SOMMAIRE

PRÉSENTATION

Face à une attaque, la technicité d'une crise cyber peut déstabiliser les plus aguerris des communicants, confrontés à des codes, des enjeux et à un écosystème parfois très éloignés de leur cœur de métier.
Tout en s'attardant sur les spécificités liées au cyber, ce guide tend à démontrer qu'une bonne communication de crise cyber reprend avant tout les réflexes et les outils communs à toute stratégie de communication de crise.

→ À QUOI SERT CE GUIDE ?

En se basant sur les situations rencontrées par l'ANSSI dans son rôle d'assistance auprès de victimes, ce guide vise à apporter des recommandations opérationnelles, pour anticiper et mettre en place une stratégie de communication de crise lors d'une cyberattaque. Si aucune recette magique n'existe en communication de crise, quelques réflexes et certaines notions essentielles peuvent être intégrés dès aujourd'hui par votre entité afin d'être prêt à faire face à une crise cyber. Ce guide, composé de dix fiches pratiques et une checklist (résumé des bonnes pratiques et pièges à éviter), contient également plusieurs témoignages de communicants d'entités publiques ou privées.

→ À QUI S'ADRESSE-T-IL ?

Ce guide s'adresse à toutes les personnes occupant une fonction de communicant lors de la gestion d'une crise dans une administration publique, une entreprise privée ou une association (ci-après nommée « entité »). Il peut s'agir d'un professionnel de la communication (directeur de la communication, chargé de communication ou agence de communication), mais parfois aussi d'autres profils (directeur/chef de cabinet, secrétaire général, juriste, etc.), faute de communicants.

→ ET D'AILLEURS, QU'EST-CE QU'UNE CRISE CYBER ?

Une crise « d'origine cyber » se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une entité (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques (cyberattaques de type rançongiciel, déni de service, etc.). C'est donc un évènement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l'entité. Par convention, on parlera ci-après de « crise cyber ».

AVANT UNE CRISE CYBER

Gérer efficacement votre communication de crise, c'est surtout l'anticiper. En amont de la crise, lorsque les temps sont plus calmes, propices à la réflexion et aux changements, des bonnes pratiques, présentes dans les fiches pratiques suivantes, sont à adopter selon le rythme propre à votre entité.

FICHE 1 AVANT UNE CRISE CYBER

INITIER UN DIALOGUE INTERNE ET ANTICIPER DES SCÉNARIOS

Lorsque survient une crise cyber, l'équipe cyber/informatique, dont le responsable de la sécurité des systèmes d'information (RSSI) et le délégué à la protection des données (DPO), et l'équipe communication sont fortement mobilisées. Faire connaissance dans ces conditions est compliqué.

Pour assurer une communication de crise cyber pertinente, il est donc indispensable d'initier un dialogue entre les équipes cyber/informatique et communication en amont. L'objectif est de mieux se connaître et de comprendre les priorités, les enjeux et le vocabulaire de chaque métier. Le responsable informatique est capable de rendre compte en temps réel de la situation technique et de ses possibles évolutions. Le communicant dispose, lui, d'une connaissance fine des cibles (interne et externe) de l'entité ainsi que des moyens de communication disponibles. Cette acculturation mutuelle peut se réaliser sous différentes formes :

- → **Ateliers de travail dédiés.**
- → **Campagnes de sensibilisation interne,** à l'occasion par exemple du Cybermois, organisé chaque année en octobre pour sensibiliser les publics européens à la cybersécurité et leur permettre d'adopter les bons réflexes.
- → **Exercices de gestion de crise cyber[1].**

[1] Pour en savoir plus, consultez le guide de l'ANSSI « Organiser un exercice de gestion de crise cyber ».

Chaque entité doit également conduire une analyse des risques[2] menaçant de déstabiliser ses activités. Les acteurs impliqués dans la gestion de crise et l'équipe cyber/informatique doivent anticiper plusieurs scénarios de crise cyber réalistes (DDoS, rançongiciel, défiguration, etc.). Il est alors recommandé de préparer des stratégies de communication de crise *(cf. Fiche 5)* en réponse aux différents scénarios identifiés qui peuvent ensuite être testées dans le cadre d'un exercice. Sans être exhaustif, l'anticipation de ces stratégies de communication permet, le jour J, d'avoir une première base sur laquelle s'appuyer pour avancer efficacement et gagner du temps.

FOCUS
LES RESSOURCES DE CYBERMALVEILLANCE.GOUV.FR

En l'absence d'une équipe cyber/informatique en interne, des prestataires ou des dispositifs comme Cybermalveillance.gouv.fr[3] peuvent donner des clés de compréhension de la cybersécurité.

[2] Pour en savoir plus, consultez la méthode EBIOS Risk Manager.
[3] La plateforme ***Cybermalveillance.gouv.fr,*** lancée en 2017, est un dispositif national de sensibilisation, de prévention et d'assistance aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales.

« L'acculturation régulière des équipes communication aux différentes formes de menaces cyber est indispensable pour faciliter la coordination lors d'une crise. »

Laurent Baude
Responsable de la communication sensible et de crise, Groupe RATP

À RETENIR

En amont d'une crise cyber, il est indispensable que les équipes communication et cyber/informatique se rencontrent afin d'avoir une meilleure compréhension mutuelle des priorités, des enjeux et du vocabulaire de chacun. Sur la base des scénarios de crise cyber probables (DDoS, rançongiciel, défiguration, etc.), il est recommandé de préparer différentes stratégies de communication.

FICHE 2 AVANT UNE CRISE CYBER

CRÉER UNE BOÎTE À OUTILS DÉDIÉE

Pour se préparer à faire face à une crise cyber, il est recommandé de rassembler en amont des ressources utiles dans une boîte à outils dédiée. Cette boîte à outils permettra de mettre en place rapidement des actions de communication de crise cyber efficaces le jour J. Celle-ci peut contenir :

- → **Les stratégies de communication de crise pré-identifiées avec les éléments de langage (EDL) associés** ***(cf. Fiches 5 et 6)*** en fonction des différents scénarios cyber probables ***(cf. Fiche 1)***. Ce document peut notamment être conçu avec l'aide du ***CyberDico*** de l'ANSSI. Ce dernier, gratuit et accessible sur le site web de l'ANSSI, liste, par ordre alphabétique, des mots, expressions et sigles du domaine de la cybersécurité. Il présente leur définition en français et en anglais et est mis à jour régulièrement.

- → **Un ordinateur vierge ou déconnecté du réseau** (pour utiliser les outils PAO ou les comptes réseaux sociaux, envoyer les communications internes, etc.).

- → **Le dispositif de gestion de crise de votre entité et les annuaires des acteurs de la cellule de crise.**

- → **Un listing des modes de communication dégradés.**
  En amont d'une crise cyber, il est crucial d'anticiper des modes de communication interne et externe dégradés car les outils habituels risquent d'être impactés voire rendus inutilisables par une cyberattaque. Pour faire cet exercice, l'imagination d'une situation extrême est requise : comment communiquer sans Internet et/ou sans accès à vos emails et/ou sans téléphone

et/ou sans accès à vos serveurs ? Vous trouverez quelques pistes de modes de communication dégradés dans la ***Fiche 8***.

→ **Les codes et outils de pilotage de la communication :**

- les codes de connexion aux comptes (réseaux sociaux, applications mobiles, site web, intranet, etc.)
- les *templates* de vos communications (communiqué de presse, publication réseaux sociaux, etc.)
- l'annuaire des porte-paroles de votre entité
- un fichier récapitulatif de vos contacts journalistes et influenceurs

Pour préparer cette boîte à outils, vous pouvez aussi utiliser le plan de reprise d'activité (PRA) ou le plan de continuité d'activité (PCA) de votre entité. Mis en place afin de réagir face à des risques identifiés, ils s'appuient sur des ressources et des procédures définies en amont des situations rencontrées.

Cette boîte à outils doit être régulièrement mise à jour avec vos retours d'expérience réels ou fictifs, issus d'un exercice de crise cyber par exemple. Elle doit être disponible sur un de vos serveurs informatiques (dans le cas où vous y avez toujours accès), une clé USB, un coffre-fort numérique et en version papier au cas où les versions numériques ne seraient plus accessibles, notamment à cause d'une cyberattaque.

> **« L'anticipation et la gestion d'une crise passent par une solide préparation et organisation des équipes ainsi que par des process définis et établis en amont. »**
>
> Caroline de Lastic
> **Directrice de la coordination stratégique et de la communication *corporate*, Naval Group**

FOCUS
LA SÉCURITÉ DE VOS COMPTES RÉSEAUX SOCIAUX EST PRIMORDIALE

→ **Choisissez un mot de passe robuste, unique pour chaque réseau social (12 caractères minimum avec majuscules, minuscules, chiffres et caractères spéciaux) et utilisez un gestionnaire de mots de passe.**

→ **Évitez de vous connecter à vos comptes réseaux sociaux depuis des réseaux Wi-Fi gratuits.**

→ **Séparez vos usages et ne connectez pas les comptes réseaux sociaux de votre entité à vos comptes personnels.**

→ **Activez systématiquement la fonctionnalité double authentification proposée par les différents réseaux sociaux, nécessitant un second facteur d'authentification (par SMS, par email, ou idéalement via l'utilisation d'une application dédiée) pour l'utilisation de tout nouvel équipement.**

→ **Procédez régulièrement à un renouvellement des mots de passe.**

→ **Évitez de conserver une trace écrite non protégée d'un mot de passe lorsqu'un partage entre collaborateurs est nécessaire.**

À RETENIR En amont d'une crise cyber, il est nécessaire de constituer une boîte à outils dédiée à la communication de crise cyber comprenant les stratégies de communication de crise cyber pré-identifiées avec les éléments de langage (EDL) associés, votre dispositif de gestion de crise, un listing des modes de communication interne et externe dégradés et vos codes et outils de pilotage de la communication.

FICHE 3 AVANT UNE CRISE CYBER

ENTRAÎNER SES ÉQUIPES

Les exercices de gestion de crise cyber sont l'occasion de tester, dans le cas d'une attaque d'ampleur paralysant votre système d'information, la maturité et la résilience de votre équipe communication ainsi que votre dispositif de communication de crise cyber. Les exercices permettent notamment d'automatiser certaines actions qui vous feront gagner du temps lors d'un incident réel, y compris en matière de communication.

Sur la base des scénarios définis avec les équipes cyber/informatique et de gestion de crise, l'organisation d'entraînements de plusieurs envergures est possible :

→ **Un exercice global dans votre entité** : ce type d'exercice vous permettra de tester la capacité de votre équipe de communicants à travailler avec l'ensemble du dispositif de gestion de crise de votre entité en cas de crise cyber. Il permettra également de tester la préparation de l'équipe communication aux différents scénarios envisagés.

→ **Un exercice uniquement dédié à la communication** : ce type d'exercice permet de familiariser votre équipe avec l'univers de la cybersécurité et de tester ses modes d'actions.

Des exercices doivent être réalisés régulièrement afin d'entraîner l'ensemble des collaborateurs (au gré des renouvellements) et de tester les nouveaux outils et procédures de votre entité. Ces derniers sont efficaces lorsqu'ils s'accompagnent en amont d'une préparation ***(cf. Fiches 1 et 2)*** et d'un retour d'expérience en aval afin de faire progresser les équipes[4] ***(cf. Fiche 9)***.

[4] Pour en savoir plus, consultez le guide de l'ANSSI « Organiser un exercice de gestion de crise cyber ».

L'organisation d'un exercice de gestion de crise cyber peut être réalisée en interne ou avec l'aide d'un prestataire spécialisé en gestion de crise[5]. Pour un entraînement réussi, il est intéressant d'y inclure de la pression médiatique simulée (PMS): faux appels médias, fausses dépêches d'agence de presse ou encore fausses publications sur de faux réseaux sociaux.

FOCUS
LE *MEDIA TRAINING*

En amont, le *media training* est une des clés de réussite de sa communication de crise cyber. Les simulations d'interviews filmées et les sessions de questions-réponses aident les porte-paroles à se familiariser avec les attentes des médias en cas de cyberattaque et à affiner leurs messages. Il permet donc de développer des réflexes qui leur seront utiles le jour du déclenchement d'une crise médiatique, alors que le temps de préparation d'une interview sera très certainement réduit.

[5] Pour en savoir plus, consultez le référentiel PACS (prestataires d'accompagnement et de conseil en sécurité des systèmes d'information).

« S'entraîner à la crise cyber, ce n'est pas craindre l'imprévu, c'est choisir de ne pas la subir. Scénarios ultra-réalistes, équipes engagées, réflexes affûtés : le jour J, on joue collectif et ça fait toute la différence ! »

Armelle Calippe
Responsable communication, relations presse et institutionnelles, France Titres – Agence nationale des titres sécurisés

À RETENIR

Il est vivement conseillé de participer à un exercice de crise cyber afin de tester la résilience de votre équipe communication et de vos outils face à une cyberattaque. Le *media training* permet aux porte-paroles de développer des réflexes qui leur seront utiles le jour du déclenchement d'une crise médiatique.

PENDANT UNE CRISE CYBER

La crise est là. La ou les cellules de gestion de crise (opérationnelle et stratégique) sont actionnées. La fonction communication s'active et vous apportez votre expertise à la gestion de la crise. Des fiches pratiques détaillent les bonnes pratiques à adopter dans les pages suivantes.

FICHE 4 PENDANT UNE CRISE CYBER

ORGANISER SA COMMUNICATION DE CRISE CYBER

Qu'il s'agisse d'une crise cyber ou non, la communication de crise doit être intégrée dès les premières heures dans le dispositif de gestion de crise de l'entité. En tant que communicant, vous avez alors plusieurs rôles à jouer et missions à remplir.

Si votre équipe communication est internalisée, une organisation spécifique de l'équipe communication en mode « crise » doit être mise en place rapidement au début de la crise cyber avec la répartition des rôles et des missions suivante.

FONCTION « COORDINATION »

Le communicant doit alors être pleinement intégré à la ou les cellules de gestion de crise afin d'aider à la prise de décision des dirigeants de l'entité sur la posture de communication. Il doit également s'assurer que la communication sortante de l'entité réponde aux objectifs définis et respecte au maximum les différents tempos des acteurs.
L'intégration du communicant aux différentes cellules permettra au démarrage et pendant la crise cyber de :

- → **Comprendre** les faits constatés, le contexte de la crise cyber et la situation en matière de communication dans laquelle se trouve l'entité ***(cf. Fiche 5).***
- → **Partager** la perception de la situation (veille médiatique et interne) pour alimenter l'analyse globale de risques de l'entité ;
- → **Définir** la posture de communication.
- → **Centraliser** les productions internes et externes et les faire valider.
- → **Faire le lien** avec les parties prenantes externes.

FONCTION « PERCEPTION »

Le communicant doit alors veiller aux réactions sur les réseaux sociaux et dans les médias sur les sujets liés à votre entité *(cf. Fiche 8)*.

→ **En amont de la crise,** le veille peut permettre de déceler des signaux faibles, notamment sur les réseaux sociaux, annonciateurs d'un incident technique (publication d'un influenceur, revendication d'un attaquant, etc.).
Dans ce cas, le communicant doit alerter les différentes parties prenantes concernées (dirigeants de l'entité, équipe cyber/informatique, etc.).

→ **Au démarrage et pendant la crise cyber,** une veille couvrant les médias et les réseaux sociaux doit être mise en place et suivie si possible par une personne dédiée. Il est également utile de suivre les éventuelles prises de parole politiques et les réactions des collaborateurs en interne (en lien avec le chargé de communication interne). Cette veille médiatique sert de base pour concevoir et adapter la posture de communication.

FONCTION « RÉACTION »

Le communicant doit alors maîtriser la diversité des publics de l'entité, qu'ils soient internes ou externes, ainsi que les outils à disposition. Cette expertise est précieuse pour garantir un bon niveau de réactivité.

→ **Au démarrage d'une crise cyber,** des messages adaptés aux différents publics, internes et externes, doivent être conçus rapidement, avec l'appui des équipes métiers concernées. Par conséquent, les communicants en charge des relations presse, des réseaux sociaux, du site web et de la communication interne adaptent et relaient les messages à leurs publics respectifs ***(cf. Fiches 7 et 8)***.

→ **Pendant la crise cyber**, la communication est vivante et s'adapte aux réactions des publics visés (cf. partie « Perception »).

Il est possible de réunir ces différentes fonctions dans une cellule dédiée à la communication de crise. Anticipez au plus tôt votre organisation de crise cyber en prévision d'un potentiel incident.

Si les effectifs de l'équipe communication sont réduits, certains de vos collaborateurs devront se charger de plusieurs rôles en même temps. S'ils sont insuffisants, il sera nécessaire de faire appel à des renforts internes ou externes. Si votre entité n'a pas d'équipe communication et/ou que sa communication est externalisée (et donc prise en charge par un prestataire), il sera alors nécessaire de vous faire accompagner sur les missions précédemment citées. Différents acteurs proposent de l'accompagnement en communication de crise cyber : des prestataires de réponse aux incidents de sécurité (PRIS) qualifiés par l'ANSSI et des agences ou des cabinets de conseil spécialisés en communication de crise. Dans le cadre des incidents suivis par le CERT-FR, un accompagnement en communication de crise cyber par l'ANSSI peut également vous être proposé.

Durant la crise cyber, il est recommandé de mettre en place une chaîne de validation hiérarchique rapide (qui alerte qui, qui tranche, etc.), un système de rotation des postes clés de l'équipe communication, voire même d'identifier des collaborateurs d'autres équipes susceptibles de venir renforcer cette équipe.

À noter : au démarrage d'une crise cyber, créer une « main courante » est un bon réflexe pour tracer les évènements liés à l'incident et les actions de communication mises en place. Chaque entrée de ce document doit contenir, a minima :

- → **L'heure et la date de l'action ou de l'évènement.**
- → **Le nom de la personne à l'origine de cette action ou ayant informé sur l'évènement.**
- → **La description de l'action ou de l'évènement.**

FOCUS
3 *SOFT SKILLS* POUR UNE BONNE GESTION DE LA COMMUNICATION DE CRISE

1

PRIVILÉGIER LE CALME

Adopter une attitude positive et calme aide à surmonter cette épreuve avec davantage de facilité. Il est aussi nécessaire de protéger au maximum l'équipe cyber/informatique des demandes des médias pour qu'elle puisse travailler sereinement.

2

FAIRE PREUVE D'AGILITÉ

Dans une situation inédite, le PCA peut ne plus suffire. Le communicant doit alors faire preuve d'agilité et penser *« out of the box »* afin d'imaginer de nouvelles façons de communiquer.

3

PRENDRE SOIN DE SOI

Une crise cyber fait souvent naître des tensions internes et un communicant peut parfois subir beaucoup de pression. Il reste donc essentiel, afin que vous puissiez mener vos missions à bien, de prendre du recul face à la situation vécue. Pour préserver votre santé, accordez-vous des moments de détente.

« La mise en place d'une cellule de crise et plus particulièrement d'une cellule communication dédiée constitue un atout majeur. Elle garantit une communication cohérente, maîtrisée et au bon niveau, élaborée en collaboration avec des experts, tandis que nos équipes cyber restent pleinement focalisées sur l'analyse et la maîtrise opérationnelle de l'incident. »

Bertrand Le Piolot
Directeur Cybersécurité Groupe,
FDJ UNITED

À RETENIR

Une organisation spécifique de crise de votre équipe communication peut être mise en place au début de la crise cyber avec une répartition des rôles (coordination, perception et réaction) et des missions. En cas de ressources en communication insuffisantes ou inexistantes, vous pouvez vous faire accompagner par des prestataires de réponse aux incidents de sécurité (PRIS), des agences ou cabinets de conseil spécialisés en communication de crise ou par l'ANSSI dans certains cas.

FICHE 5 PENDANT UNE CRISE CYBER

DÉFINIR SA STRATÉGIE DE COMMUNICATION DE CRISE CYBER

1 ÉTAT DES LIEUX

Il n'existe pas de stratégie de communication unique en réponse à une crise cyber. La stratégie adaptée dépend notamment des faits, de la situation en matière de communication mais également du contexte au moment de la crise cyber. Au début d'une crise cyber, le communicant doit ainsi réaliser un état des lieux en obtenant les informations essentielles ci-après.

FAITS CONSTATÉS

→ **Demandez un point de situation pour comprendre l'incident, car il existe différents types de cyberattaques.** Essayez d'en savoir plus sur les impacts de l'incident sur les métiers et les services/outils. L'objectif est de savoir si l'attaque en elle-même est visible pour vos publics interne et externe (exemple : un rançongiciel ou un déni de service sont très visibles, contrairement à une opération d'espionnage) ou si les impacts de cette attaque sont visibles (exemple : l'impossibilité pour l'entité de payer ses collaborateur ou de maintenir ses services habituels).

→ **Résumez les premières actions entreprises par votre entité sur l'ensemble des volets** : technique, juridique, communication et même organisationnel.

SITUATION EN MATIÈRE DE COMMUNICATION

→ **Faites un point sur la stratégie de communication globale de votre entité** pour définir une stratégie de communication de crise cohérente avec l'identité de votre entité, ses objectifs et ses cibles prioritaires.

→ **Dressez un état des lieux des canaux de communication qui restent disponibles malgré la cyberattaque** (réseaux sociaux, site web, messagerie interne, etc.) ou avec des contraintes fortes (exemple : canaux accessibles seulement sur des postes déconnectés).

→ **Demandez un point de situation de la perception du sujet en interne, dans les médias et sur les réseaux sociaux** reprenant notamment les premières réactions des collaborateurs, des clients, des usagers ou des fournisseurs). Une cyberattaque peut connaître une viralité forte et de nombreux « experts » sur les réseaux sociaux ou journalistes spécialisés peuvent réagir rapidement et publiquement.

→ **Prenez en considération le nombre de demandes presse reçues** par votre service presse et les thématiques abordées.

→ **Demandez à votre délégué à la protection des données (DPO) ou votre service juridique si vous avez des obligations légales qui peuvent obliger votre entité à informer des parties prenantes** (par exemple au titre du Règlement général sur la protection des données [RGPD] dans le cas d'un vol de données). Cette information prévue par une disposition légale est à réaliser en sus de la communication publique de crise et peut impacter notamment le *timing* de communication.

→ **Identifiez si des parties prenantes ont déjà communiqué sur votre incident.** Il peut s'agir de la Commission nationale de l'informatique et des libertés (CNIL), de la section J3 Cybercriminalité du Parquet de Paris, d'autorités de régulation ou sectorielle, de vos clients, usagers, partenaires ou prestataires ou dans de très rares cas, de l'ANSSI. Des personnalités politiques peuvent également communiquer sur des crises cyber, allant parfois jusqu'à se déplacer auprès des victimes.

→ **Évaluez la visibilité des attaquants.** Certains groupes d'attaquants se distinguent par des stratégies de communication spécifiques, comme la revendication automatique de leurs attaques ou la menace de publication des données exfiltrées. Ces actions peuvent être plus ou moins visibles en fonction du canal de communication privilégié par l'attaquant. Ce dernier peut communiquer sur un site vitrine sur le *dark web*, via une messagerie chiffrée voire même avec un communiqué de presse ou sur les réseaux sociaux. Ayez également à l'esprit que les attaquants peuvent contacter directement des journalistes, des collaborateurs ou différents services de votre entité dont votre service de presse (interne ou externalisé chez un prestataire) par email ou par téléphone, afin d'accroître la pression et forcer une réaction précipitée de la victime.

CONTEXTE

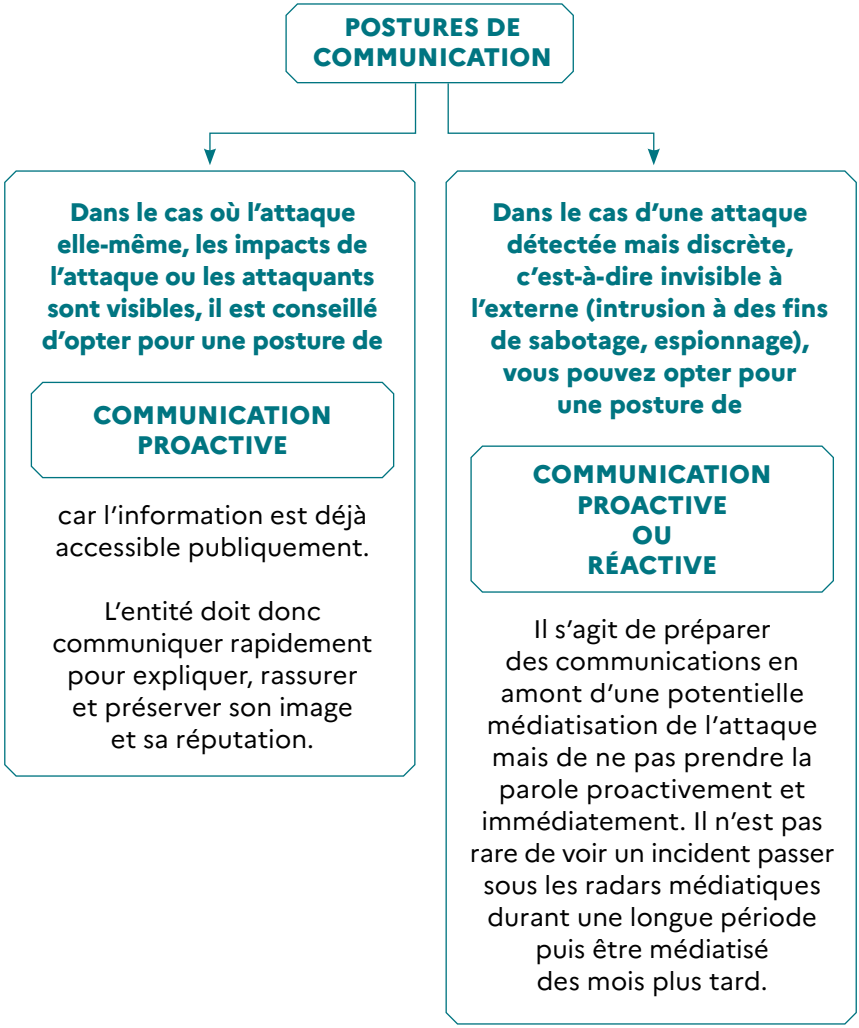
Identifiez d'éventuels points de vigilance liés au contexte dans lequel vous vous inscrivez :

→ **L'actualité de votre entité.** Par exemple : une importante campagne de communication qui débute bientôt, la publication prochaine des résultats financiers, des négociations salariales en cours, le lancement à venir d'un produit, voire même le rachat de votre entité.

→ **L'actualité socio-économique et politique entourant votre entité**, avec un évènement sectoriel majeur en préparation ou une période électorale en cours ou à venir.

2 POSTURE DE COMMUNICATION

Une fois l'état des lieux réalisé, vous devez définir et proposer à vos dirigeants une posture de communication (proactive ou réactive) à adopter.



Gardons en tête que le communicant ne fait que proposer une posture de communication qui s'intègre dans une analyse coûts/bénéfices (humains, financiers, juridiques, réputationnels, etc.) globale élaborée avec l'ensemble des parties prenantes de l'entité. Le choix de la posture revient aux dirigeants avec une prise de risques à court et moyen terme assumée.

Cette posture de communication doit être réévaluée tout au long de la gestion de la crise cyber au regard du contexte évolutif de l'incident afin de réorienter les actions de communication en conséquence.

« Les crises cyber, par leur interdépendance et leur immédiateté, exigent une communication fondée sur l'objectivité et la pédagogie, structurée autour d'une stratégie pluridimensionnelle impliquant l'ensemble des parties prenantes de l'entreprise. »

Marie-Laure Fraux
Conseillère Communication,
Banque de France

FOCUS
COMMUNIQUER SUR UNE CYBERATTAQUE À DES FINS LUCRATIVES

Un rançongiciel – *ransomware* en anglais – est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Les rançongiciels figurent au catalogue des outils auxquels ont recours les cybercriminels motivés par l'appât du gain.
Lors d'une attaque par rançongiciel, l'attaquant met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible ou irréversible. En pratique, la plupart des rançongiciels chiffrent par des mécanismes cryptographiques les données de l'ordinateur ou du système, rendant leur consultation ou leur utilisation impossibles. L'attaquant adresse alors un message non chiffré à la victime où il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.
Ce type d'attaque présente deux caractéristiques propres, différentes d'attaques plus discrètes :

LE TEMPO
visibilité quasi immédiate et systématique de l'attaque

Une attaque par rançongiciel a de très grandes chances d'être rendue publique rapidement, en raison des impacts de la cyberattaque (exemple : impossibilité de rendre un service aux clients ou usagers), d'une fuite d'informations sur la base de captures d'écran de l'entité partagées à l'externe ou de certains groupes cybercriminels qui développent leur propre communication publique autour de l'attaque pour faire davantage pression sur la victime (chantage pour le déchiffrement, la publication d'un échantillon ou la revente des données).

LES OUTILS
paralysie possible des outils classiques de communication

En fonction de la propagation de l'incident, les outils bureautiques peuvent être partiellement ou complètement indisponibles, empêchant l'accès aux outils de travail du communicant (fichier presse, accès aux comptes des réseaux sociaux ou au site Internet, emails, etc.) et la mise en œuvre d'actions de communication rapide (email ou message interne, emails clients/usagers, etc.).

Ces deux caractéristiques obligent le communicant à opter le plus souvent pour une posture de communication proactive dès les premières heures de l'incident pour limiter les impacts de la crise cyber sur l'image et la réputation de l'entité, tant en interne qu'en externe.

FOCUS
COMMUNIQUER SUR UNE ATTAQUE À DES FINS D'ESPIONNAGE

Une attaque cyber n'est pas forcément visible. Discrètes et plus sophistiquées, les attaques à des fins d'espionnage ont des conséquences parfois désastreuses. Des attaquants peuvent s'introduire dans les systèmes d'information, parfois pendant plusieurs années, afin notamment de voler des données stratégiques.

Pour ce type d'attaque, détectée parfois par hasard ou très tardivement, la remédiation est souvent longue, l'attaquant pouvant disposer de droits élevés sur le système d'information. Il faudra alors prévoir des actions techniques en profondeur pour éjecter l'attaquant et renforcer la sécurité du système d'information. Réagir face à une cyberattaque de ce type, c'est également entamer une interaction avec un adversaire : les actions de votre entité et leurs effets peuvent être observés et interprétés par l'attaquant. Sa réaction est variable selon son niveau de compétence, de persistance et d'agressivité.

La communication doit donc être abordée différemment pour ce type d'attaque car les échanges, qu'ils soient internes ou externes (entre les gestionnaires de la crise, avec les équipes de l'entité ou avec des partenaires, clients/usagers ou prestataires) sont des sources d'information potentielles pour l'attaquant. Il est donc nécessaire de « cacher son jeu » en contrôlant les informations perceptibles par l'attaquant afin de limiter ses possibilités d'adaptation ou de réaction.

Votre posture de communication, généralement réactive, est définie en fonction du niveau de précaution à prendre dans les actions de remédiation pour les protéger de la vue de l'adversaire. Concernant la communication interne, elle doit être mesurée afin de ne pas compromettre les actions de remédiation en cours. Pour la communication externe, il est conseillé de ne pas communiquer en amont de l'éviction définitive de l'attaquant du système d'information mais des messages clés doivent être néanmoins préparés (sans qu'ils soient hébergés dans votre système d'information) et prêts à être diffusés.

Il est recommandé de se référer au guide de l'ANSSI « Cyberattaques et remédiation : préparer la remédiation » pour un développement dédié à ce sujet.

FOCUS
COMMUNIQUER SUR UNE ATTAQUE À DES FINS DE DÉSTABILISATION

Certaines attaques informatiques, telles que le déni de service distribué (DDoS) ou la défiguration de site Internet, ont pour objet principal la déstabilisation de l'entité visée. Un DDoS a pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. L'action peut être malveillante ou être la conséquence d'un mauvais dimensionnement du service. On parle de déni de service distribué lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés. La défiguration est le résultat d'une activité malveillante qui a modifié l'apparence ou le contenu d'un serveur Internet et a donc transgressé l'intégrité des pages en les altérant.

Ces attaques ont des impacts métiers réels, provoquant un dysfonctionnement des services proposés, avec un coût financier parfois non négligeable. Cependant, peu sophistiquées, elles peuvent être détectées et stoppées assez rapidement et elles n'engendrent généralement pas d'impacts à long terme (comme la perte de données ou la destruction du système d'information). Elles ont toutefois un effet symbolique et émotionnel très important : elles mettent en lumière la vulnérabilité d'un service, voire servent d'étendard pour des attaquants aux messages anxiogènes.

Dans ce type d'attaque peu sophistiquée ou lors d'un « faux incident », cela peut générer une crise médiatique plus importante à gérer que la partie technique de l'incident lui-même.

La posture de communication proactive est alors fondamentale : elle vise à expliquer de façon pédagogique les impacts réels de l'attaque, généralement modérés, afin de rassurer rapidement les publics mobilisés sur la question. En l'absence d'une communication adaptée et mesurée, ces attaques peuvent atteindre leur but final de déstabilisation en provoquant un emballement médiatique.

3 OBJECTIFS DE COMMUNICATION

Une fois l'état des lieux réalisé et la posture choisie, vous pouvez définir vos objectifs de communication. Vous trouverez ci-après les principaux objectifs de communication à atteindre lors d'une crise cyber :

EXPLIQUER ET INFORMER

Faire de la pédagogie sur le type d'attaque auquel l'entité est confrontée et les actions de remédiation qui en découlent afin d'améliorer la compréhension des évènements et le partage de connaissance.

RASSURER

Montrer que votre entité fait le nécessaire pour sortir rapidement de la crise cyber afin de conserver la confiance de ses clients ou de ses usagers mais aussi de l'interne.

PRÉSERVER L'IMAGE ET LA RÉPUTATION DE L'ENTITÉ

Limiter les impacts sur la notoriété de l'entité grâce à une communication transparente ***(cf. Fiche 9)***.

Il est également nécessaire de s'assurer de la non propagation de rumeurs ou de fausses informations ***(cf. Fiche 8)***.

FAIRE CHANGER LES COMPORTEMENTS

Inciter les collaborateurs à adopter des bonnes pratiques de sécurité numérique dans leurs futurs usages.

4 CIBLES

Lors d'une crise cyber, on retrouve habituellement les cibles de communication suivantes :

INTERNES

- → **Collaborateurs** (ou uniquement ceux dont les données sont exfiltrées voire publiées dans le cas d'un vol de données)
- → **Managers, CODIR/COMEX, dirigeants**
- → **Prestataires travaillant en interne**
- → **Filiales ou entités parentes**
- → **Instances représentatives du personnel** (comité social et économique, syndicats, représentants du personnel, etc.)
- → **Porte-paroles**

EXTERNES

- → **Journalistes** (nationaux et régionaux, généralistes ou spécialisés en cybersécurité/tech ou dans le secteur impacté)
- → **Influenceurs cyber et du secteur impacté**
- → **Prospects**
- → **Clients** (cible qui peut être divisée en deux cercles, les clients VIP et le reste des clients)
- → **Usagers**
- → **Prestataires**
- → **Fournisseurs**
- → **Actionnaires et membres du Conseil d'Administration**
- → **Partenaires** (français, européen et internationaux)
- → **Grand public**
- → **Personnes dont les données sont exfiltrées voire publiées** (dans le cas d'un vol de données)
- → **L'ANSSI et le CERT-FR,** notamment si vous êtes soumis à des obligations réglementaires
- → **Autorités sectorielles**

→ **Autorités politiques ou de tutelles, cabinets ministériels**
→ **Homologues techniques** (CSIRT sectoriel, ministériel ou territorial, InterCERT France, CERT-EU)
→ **CNIL**
→ **Section J3 Cybercriminalité du Parquet de Paris**

Si certaines de vos parties prenantes sont à l'international (collaborateurs, clients, usagers, etc.), gardez à l'esprit l'enjeu de traduction rapide des contenus (a minima en anglais).

Attention, un communicant n'a pas vocation à centraliser la rédaction et l'envoi des communications à l'ensemble des cibles ! Le rôle du communicant est de coordonner les différentes prises de parole pour rendre la communication globale de l'entité cohérente, claire et maîtrisée. Chaque acteur joue donc son rôle, dans le cadre de ses attributions, mais avec une vision collective, partagée et validée.

5 TEMPO DE COMMUNICATION

Le tempo d'une crise cyber est toujours difficile à expliquer : si l'attaque ou les impacts sont parfois immédiatement visibles, les analyses techniques prennent du temps, tout comme les mesures de remédiation. Cet argument, bien que frustrant, est généralement bien compris des médias spécialisés en cybersécurité mais moins bien par vos autres cibles. Il est nécessaire d'avoir à l'esprit quelques conseils en matière de tempo de communication.

DANS LE CAS D'UNE POSTURE DE COMMUNICATION RÉACTIVE

→ Questionnez le moment et la pertinence de votre première communication interne et/ou externe, en fonction de l'état des lieux (les faits, la situation en matière de communication et le contexte au moment de la crise cyber).

DANS LE CAS D'UNE POSTURE DE COMMUNICATION PROACTIVE

→ **Communiquez rapidement** car dans la société actuelle, les réseaux sociaux et les chaînes d'informations en continu ont fait de l'instantanéité de la diffusion des informations une caractéristique essentielle de la communication de crise. Au début de la crise cyber, vous disposez de très peu d'informations vérifiées. Votre première communication peut alors être courte et se limiter à indiquer que vous avez connaissance de l'incident et que vos équipes sont mobilisées pour le gérer. Dans tous les cas, ne communiquez jamais des informations non vérifiées, elles risquent de se retourner contre vous et de générer un *bad buzz*.

→ **Évitez de donner une date de retour à la normale précise au début de l'incident** car des imprévus sont toujours possibles (exemples : l'attaquant revient et lance un rechiffrement, les équipes cyber/informatique sont confrontées à des difficultés techniques lors de la remédiation, etc.). Vous pouvez **informer régulièrement vos différentes parties prenantes** pendant la crise cyber en donnant de la visibilité sur les étapes des investigations et de la remédiation (dès que cette dernière est maîtrisée).

→ **Priorisez les communications en fonction de vos cibles** en communiquant notamment auprès de vos collaborateurs et clients/usagers avant de réaliser un communiqué de presse.
→ Dans la mesure du possible et sans que cela complexifie la situation pour votre entité, **occupez l'espace médiatique**, pour éviter que d'autres acteurs (experts, influenceurs, prestataires, clients, usagers, concurrents) ne s'expriment à votre place.

FOCUS
COMMUNIQUER SUR UNE EXFILTRATION DE DONNÉES PERSONNELLES

L'exfiltration de données est le vol ou le transfert non autorisé des données depuis un terminal ou un réseau vers une machine extérieure maîtrisée par un acteur malveillant. Une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable, qui doit donc pouvoir en conserver la maîtrise. Une personne physique peut être identifiée directement (exemples : nom et prénom) ou indirectement (exemples : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou email, mais aussi par la voix ou l'image).

Une cyberattaque permettant d'exfiltrer des données personnelles est souvent suivie d'un chantage au déchiffrement, de la publication d'un échantillon et de la revente en source ouverte de ces données par l'attaquant.

Ce type d'attaque, par nature visible, a la plupart du temps un impact réputationnel significatif et peut susciter une grande inquiétude de la part de vos clients ou usagers et partenaires. De plus, selon la nature des données concernées, des sollicitations importantes peuvent émaner des médias nationaux ou étrangers et les commentaires sur les réseaux sociaux peuvent être nombreux. Ce type d'attaque nécessite donc une communication de crise adaptée.

Si un attaquant publie un échantillon de données qu'il désigne comme étant les vôtres, il est nécessaire de communiquer en plusieurs étapes.

1re COMMUNICATION

Rapidement après la publication des données exfiltrées par l'attaquant, l'ANSSI conseille d'indiquer publiquement que vous avez pris connaissance de ce potentiel incident touchant votre entité. Indiquez qu'une qualification des données est en cours afin de confirmer ou non qu'elles vous appartiennent réellement.

3e COMMUNICATION

En cas de risque élevé pour les droits et libertés d'une personne physique, l'entité victime doit informer individuellement du vol de données à caractère personnel les personnes concernées dans les meilleurs délais. Vous trouverez dans ***l'article 34 du Règlement général sur la protection des données (RGPD)*** les conditions à remplir. Assurez-vous également que les personnes concernées puissent par ailleurs vérifier la légitimité de l'information reçue. L'information aux personnes concernées doit être individuelle par défaut, et sous dérogation peut être remplacée par une communication publique. Pour en savoir plus sur les dérogations prévues, veuillez vous référer à l'article 34 du RGPD.

2e COMMUNICATION

Si les données exfiltrées n'appartiennent pas à votre entité, un démenti public sera alors nécessaire. Si les données exfiltrées appartiennent réellement à votre entité, confirmez l'exfiltration et la publication de données personnelles en ajoutant également un mot d'excuse vis-à-vis du dommage occasionné aux personnes concernées.
Vous devez préciser si les données exfiltrées appartiennent à votre entité ou si ce sont des données de clients stockées par vos soins (dans le cas où vous êtes un sous-traitant). Si c'est le cas, il est important de préciser les mesures prises vis-à-vis des autorités : alerte de l'incident à l'ANSSI, dépôt de plainte auprès des services de police ou de gendarmerie spécialisés, la notification initiale et/ou complémentaire auprès de la CNIL. Pour réaliser une notification, rendez-vous sur ce site ***notifications.cnil.fr/notifications*** et vous pouvez également poser vos questions à ***violations@cnil.fr***.
Indiquez également qu'une qualification précise des données est en cours pour déterminer leur nature et qu'un retour vers les personnes concernées par cette exfiltration sera fait, le cas échéant.

À RETENIR

Il n'existe pas de stratégie de communication unique en réponse à une crise cyber. La stratégie adaptée dépend notamment des faits constatés, de la situation en matière de communication mais également du contexte. Au début d'une crise cyber, le communicant doit proposer à ses dirigeants une posture de communication à adopter : proactive ou réactive. Expliquer, informer, rassurer, préserver l'image et la réputation de l'entité et faire changer les comportements sont les objectifs de communication principaux. Il existe également plusieurs cibles à définir et à adresser aussi bien en interne (collaborateurs, managers, représentants du personnel, etc.) qu'en externe (journalistes, usagers, clients, actionnaires, partenaires, autorités, etc.). Concernant le tempo, le temps de l'analyse et de la remédiation de l'incident n'est pas aligné avec le temps médiatique. En cas de communication réactive, le communicant doit questionner le moment et la pertinence d'une première communication. En cas de communication proactive, le communicant doit communiquer rapidement uniquement des informations vérifiées, ne pas s'engager sur une date de retour à la normale précise, informer régulièrement et occuper l'espace médiatique si cela est possible. Il est également indispensable de prioriser les communications en fonction de vos cibles et notamment en informant en premier lieu vos collaborateurs et vos clients/usagers.

FICHE 6 PENDANT UNE CRISE CYBER

RÉDIGER LES MESSAGES CLÉS

1 INFORMATIONS FACTUELLES ET VÉRIDIQUES

Le sujet cyber est aujourd'hui fortement suivi par une communauté dédiée. Cette communauté cyber est composée d'influenceurs au sens large et de journalistes exigeants, qui aiment comprendre les modes opératoires des attaquants. Elle est très active sur les réseaux sociaux pour alerter sur des incidents, échanger sur des éléments techniques et commenter les revendications d'attaquants et parfois les communications officielles. La communauté cyber garde en mémoire les incidents et peut, même plusieurs mois après, revenir sur la manière dont ils ont été gérés y compris en matière de communication. Toute communication en période de crise est donc observée avec attention.

C'est pourquoi votre communication doit d'abord être **véridique**. Comme pour toute communication de crise, mentir est fortement déconseillé. Vous n'êtes pas obligé de tout dire, à chaque instant et à tout le monde, mais tout ce que vous dites doit être vrai. L'objectif est de faire preuve d'une transparence maîtrisée, par exemple en communiquant des points de situation réguliers. Si vous mentez ou refusez de communiquer, vos parties prenantes en déduiront que vous avez quelque chose à cacher et feront leurs propres suppositions, ce qui peut amplifier la crise médiatique en cours.

Si vous émettez des hypothèses à un instant T, précisez qu'il faut les entendre comme telles et employez le conditionnel. Par exemple : « à ce stade des investigations, aucune donnée personnelle n'aurait été compromise. Nos équipes poursuivent les analyses pour confirmer ce résultat. »

Votre communication doit également être **factuelle** : évitez les jugements de valeur. Ne minimisez/exagérez pas volontairement ou involontairement la sophistication de l'attaque subie car la supercherie sera vite découverte. Il est donc nécessaire de se baser sur les évaluations de votre équipe technique.

Enfin, il est conseillé de faire relire et valider vos messages par la cellule de crise stratégique.

FOCUS
LES FAKES NEWS

La quantité d'énergie nécessaire pour réfuter des mensonges est supérieure à celle nécessaire pour les produire. Cependant, lors d'une crise cyber, il est impératif de corriger les fausses informations publiées en interne comme en externe par les collaborateurs, internautes, journalistes, bots, etc.

2 TON ET VOCABULAIRES EMPLOYÉS

Lors de l'élaboration de vos messages, portez une attention particulière au vocabulaire et au ton employés. Le ton de votre communication doit être pédagogique, rassurant, et peut bien sûr évoluer avec la crise. Concernant le vocabulaire à adopter :

→ **Évitez les termes trop anxiogènes** : la cyberattaque est déjà génératrice de stress, il n'est donc pas nécessaire d'en rajouter.

→ **Adaptez la technicité de vos messages en fonction du public ciblé** : la cybersécurité est par essence technique et connaît des évolutions technologiques rapides. Ainsi, si vous vous adressez à un lectorat non expert, il faudra vulgariser vos messages au maximum et définir les mots les plus complexes lorsque ceux-ci sont indispensables. A contrario, les points de situation transmis notamment à un centre de réponse aux incidents cyber (CSIRT) pourront adopter un vocabulaire technique adapté. Évitez également le jargon employé au sein de votre entité.

Pour vous aider dans la rédaction de vos supports, vous pouvez utiliser le CyberDico de l'ANSSI, gratuit et accessible sur le site Internet de l'Agence. Ce document de référence, liste, par ordre alphabétique, des mots, expressions et sigles du domaine de la cybersécurité. Il présente leur définition en français et en anglais et est mis à jour régulièrement.

FOCUS SUR L'EMPATHIE ET L'HUMOUR

Opposer ou apporter uniquement des arguments factuels à une émotion collective est complexe. Un message d'empathie et d'excuse est indispensable en cas de cyberattaque (surtout si des personnes sont directement touchées, dans le cas d'un vol de données par exemple). De plus, opter pour l'humour afin d'alléger les tensions est déconseillé : la perception de l'incident est très différente en fonction des personnes. L'humour peut être perçu comme le signe d'une gestion légère ou déconnectée de la réalité, en contradiction avec la criticité et le stress vécu par certains acteurs.

3 ÉLÉMENTS DE LANGAGE ADAPTÉS

Pour vous aider à élaborer le contenu de votre communication, vous pouvez utiliser la grille ci-après. Cette dernière présente à la fois :

- → **Une structuration selon la méthode FACET** (F pour Faits, A pour Actions, C pour Compassion, E pour Engagement et T pour Transparence) pour rédiger vos communiqués de presse, publications réseaux sociaux ou actualités web.
- → **Les questions qui sont habituellement posées en cas de crise cyber.**
- → **Des conseils pour écrire vos éléments de langage proactifs ou réactifs.**

> **« En pleine crise cyber, la réactivité en termes de communication interne comme externe est clé. Il est essentiel d'établir rapidement des éléments de langage clairs, précis et partagés afin de reconnaître et d'expliquer la situation et prévenir ainsi rumeur et emballement médiatique. »**
>
> François Lecerf
> **Directeur Commercial & Marketing,**
> **Groupe LGM**

FAITS

POTENTIELLES QUESTIONS POSÉES PAR VOS PARTIES PRENANTES	CONSEILS POUR ÉCRIRE VOS EDL PROACTIFS
De quel type d'attaque s'agit-il ?	Il est préférable de parler « d'incident de cybersécurité » ou de « cyberattaque » plutôt que de « piratage informatique » pour être moins anxiogène. Dans le cas où l'attaque n'a pas abouti, vous pouvez indiquer une « tentative d'intrusion sur votre système d'information ». S'il s'agit d'un problème technique et non d'une cyberattaque, il est important de l'indiquer en employant le terme de « panne technique » par exemple.
Quel est le vecteur d'attaque ?	Il existe différents vecteurs d'attaque : « informations d'identification compromises », « logiciels malveillants », « hameçonnage », « DDoS », « exploitation d'une vulnérabilité » ou d'une « vulnérabilité *zero-day* », etc. Les définitions de ces termes sont à retrouver dans le CyberDico de l'ANSSI. En interne comme en externe, limitez au strict minimum le partage des détails techniques sur la manière dont s'est passée l'attaque. Ils ne sont pas utiles pour vos publics et cela risquerait de donner des informations aux attaquants, s'ils sont toujours présents dans votre système d'information ***(cf. Fiche 5)***.
Quelles sont les conséquences directes ou indirectes de la cyberattaque ?	Les conséquences peuvent être techniques, organisationnelles ou financières, sur la structure, les services ou les produits de votre entité. Il est également crucial d'indiquer s'il y a eu ou non une latéralisation de l'attaque à des entités partenaires ou clientes.
Est-ce qu'il y a eu une exfiltration de données ?	Dans le cas d'un potentiel vol de données, référez-vous à la ***Fiche 5***.
Quand est-ce que l'incident est arrivé ?	Vous devez indiquer une date plus ou moins approximative du début de l'attaque et/ou de détection de l'incident (exemples : « dans la nuit de vendredi à samedi », « ce matin »). Cet exercice est plus complexe à réaliser dans le cadre d'une attaque de type espionnage ou sabotage, car la compromission a souvent eu lieu plusieurs mois ou années avant d'être détectée. Dans ce cas, vous pouvez uniquement indiquer la date de détection de l'incident.
L'attaque est-elle toujours en cours ?	Si l'attaque est finie, il est possible de répondre à cette question en indiquant qu'« à la suite de nos investigations et de nos actions d'endiguement et de remédiation, nous n'observons plus de trace de l'attaquant dans le système d'information ».

ACTIONS

POTENTIELLES QUESTIONS POSÉES PAR VOS PARTIES PRENANTES	CONSEILS POUR ÉCRIRE VOS EDL PROACTIFS
Quelles sont les actions mises en œuvre ?	Il est indispensable de mettre en avant : ▸ Les actions mises en œuvre pour stopper la cyberattaque et rétablir au plus vite les produits ou services affectés (par exemple : isolation du réseau, coupure temporaire de certains services, déconnexion des accès clients/tiers pour les protéger, durcissement de certains accès, etc.). ▸ La mise en place d'une cellule de crise. ▸ Les services ou produits affectés ou non par la cyberattaque. ▸ La continuité des activités en mode normal ou dégradé. ▸ Les contacts en cas de question (par exemple : adresse mail générique ou numéro vert).
Êtes-vous accompagné par l'ANSSI ?	Le cas échéant, vous pouvez indiquer que : ▸ Vous avez prévenu l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de la situation ; ▸ Vous êtes accompagné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour traiter votre incident. Cette mention doit faire l'objet d'une validation par l'ANSSI : cert-fr@ssi.gouv.fr.
Êtes-vous accompagné par des prestataires ?	La mention de l'accompagnement de votre entité par des experts en cybersécurité privés (prestataire de réponse à incidents - PRIS) ou par des CSIRT (sectoriel, territorial ou ministériel) est recommandée pour rassurer vos publics.

ACTIONS

Est-ce que les collaborateurs, clients ou usagers ont des mesures à prendre ? **Peuvent-ils bénéficier de bonnes pratiques ?**	Dans vos différentes communications, vous pouvez transmettre des consignes pratiques à vos collaborateurs, clients ou usagers : ▸ Demander expressément à ne pas surcharger les lignes téléphoniques du service informatique de votre entité déjà mobilisé sur l'incident. ▸ Donner des consignes techniques ou organisationnelles pour que les collaborateurs puissent continuer à travailler. ▸ Transmettre des bonnes pratiques de cybersécurité, comme le changement des mots de passe, la mise en place de la double authentification ou la forte vigilance sur les emails reçus.
Quelles mesures ont été prises vis-à-vis des autorités ? **En cas de vol de données personnelles, une notification auprès de la CNIL a-t-elle été réalisée ?** **Une plainte auprès des services de police ou de gendarmerie spécialisés a-t-elle été déposée ?**	Le cas échéant pour montrer votre capacité à gérer correctement votre crise cyber : ▸ Indiquez dans votre communication que vous avez réalisé une notification initiale et/ou complémentaire auprès de la CNIL et spécifiez, le cas échéant, que les personnes concernées ont été/seront informées individuellement (et spécifier le canal si connu). ▸ Précisez qu'un dépôt de plainte a eu lieu. Cette judiciarisation aura pour conséquence de limiter vos actions de communication car certains éléments précis de l'attaque ne pourront pas être dévoilés sans l'accord préalable du service enquêteur.

COMPASSION

POTENTIELLES QUESTIONS POSÉES PAR VOS PARTIES PRENANTES	CONSEILS POUR ÉCRIRE VOS EDL PROACTIFS
Est-ce que votre entité a un mot pour les victimes de cet incident ?	Il convient de s'adresser, en faisant preuve de compassion, non seulement aux victimes directes de la crise, mais également à tous ceux qui pourraient se considérer comme telles. La méthode FACET devient CAFET (C pour Compassion en premier et les Faits après les Actions) lorsque la crise fait des victimes physiques (blessés ou décès). Dans ce cas, la compassion à leur égard passe avant toute autre considération.

ENGAGEMENT

POTENTIELLES QUESTIONS POSÉES PAR VOS PARTIES PRENANTES	CONSEILS POUR ÉCRIRE VOS EDL PROACTIFS
Quel est le niveau de prise en compte de cet incident au sein de votre entité ?	Il est nécessaire de montrer que votre entité a réagi rapidement et efficacement et est fortement mobilisée pour gérer l'incident, avec notamment la mise en place d'une cellule de crise. Vous pouvez aussi rappeler que la sécurité des systèmes d'information et la protection des données personnelles sont au cœur de vos priorités.
Quelles mesures allez-vous mettre en place à l'avenir ?	Vous pouvez indiquer les actions déjà réalisées en matière de cybersécurité de votre système d'information ces dernières années et les enseignements tirés de cette crise cyber (exemple : la mise en place d'un plan d'action supplémentaire ou le déblocage d'un budget dédié à la cybersécurité).

TRANSPARENCE

POTENTIELLES QUESTIONS POSÉES PAR VOS PARTIES PRENANTES	CONSEILS POUR ÉCRIRE VOS EDL PROACTIFS
Combien de temps cela va-t-il durer ? **Quelles sont les prochaines étapes à venir jusqu'à la sortie de la crise ?** **À quand un retour à la normale ou à un fonctionnement optimal ?**	Vous devez faire de la pédagogie sur le temps que nécessitent les investigations et la remédiation. Les analyses techniques sont souvent longues, la remédiation peut prendre du temps et des surprises peuvent arriver. Ne vous engagez pas au début de la crise sur une date précise de retour à la normale mais donnez plutôt de la visibilité à chaque étape des investigations ou de la remédiation ***(cf. Fiche 5)***. Les éléments ci-après peuvent être utilisés : « La durée de l'indisponibilité des produits et services, tout comme le calendrier de retour à la normale ne sont pas encore déterminés. » « Le service est momentanément indisponible. »
Quand partagerez-vous de nouvelles informations ?	Pour répondre à cette question, vous pouvez indiquer que les investigations et la remédiation continuent et que de nouvelles informations seront communiquées dès qu'elles seront disponibles. Par exemple : « Nous continuerons à informer régulièrement nos différentes parties prenantes au fur et à mesure de l'avancée de nos investigations et de la remédiation. ».
Qui contacter en cas de questions ?	En interne comme en externe, il est nécessaire de protéger la cellule de crise et les équipes techniques de nombreuses sollicitations incommodantes avec « un cordon sanitaire » pour leur permettre de se focaliser sur la résolution de l'incident. Vous pouvez par exemple mettre en visibilité un formulaire de contact ou une adresse email générique créée pour l'occasion, mais cela nécessitera de gérer les demandes qui pourront être nombreuses. Il est également possible d'activer un numéro vert pour traiter un grand nombre d'appels. En interne, il est conseillé de cadrer clairement au début de la crise les échanges avec les médias. Demandez aux collaborateurs de renvoyer les demandes presse vers votre service de presse, dans le cas où ils seraient contactés par des journalistes, afin de centraliser la gestion des relations presse.

Les éléments suivants sont des sujets que l'ANSSI recommande d'aborder uniquement de manière réactive.

POTENTIELLES QUESTIONS POSÉES PAR VOS PARTIES PRENANTES	CONSEILS POUR ÉCRIRE VOS EDL PROACTIFS
Qui est l'attaquant ? **Quelles sont ses motivations ?**	Les autorités françaises distinguent l'imputation d'une attaque informatique (à un mode opératoire ou à un groupe d'attaquants) de l'attribution politique à un commanditaire identifié. ▸ Les attaquants peuvent facilement tenter de se faire passer pour ceux qu'ils ne sont pas en réalisant parfois des fausses revendications, ou en laissant de fausses traces sur leur passage pour brouiller les pistes. L'imputation d'une attaque informatique se concentre sur la caractérisation technique des outils, des techniques et des tactiques de l'attaquant afin de déterminer ses intérêts et ses méthodes de travail, de le relier à des cyberattaques connues, et enfin, d'identifier un groupe d'attaquants ou un commanditaire. Ce travail technique, auquel un niveau de certitude variable est accordé, sert ensuite de base de décision pour une éventuelle attribution. ▸ L'attribution publique d'une attaque informatique est une décision politique, prise au plus haut niveau de l'État, qui vise à désigner le groupe d'attaquants ou le commanditaire, généralement un État, comme responsable de cette attaque. C'est pourquoi, même si les médias vont rapidement vous demander qui est derrière la cyberattaque que vous subissez, il est vivement conseillé de ne pas indiquer publiquement d'informations sur les attaquants. Cela vous évitera de vous tromper, de faire la publicité des attaquants ou bien d'ajouter une dimension géopolitique à votre crise, qui sera difficilement maîtrisable.

Avez-vous reçu une demande de rançon et si oui, avez-vous payé la rançon ?	Si la demande de rançon est déjà publique, vous pouvez la confirmer dans vos messages. L'ANSSI recommande de ne jamais payer la rançon. En effet, le paiement d'une rançon ne garantit pas l'obtention d'un moyen de déchiffrement ou, dans le cas de l'obtention de ce dernier, de reconstituer l'intégralité des fichiers chiffrés. Il ne permettra pas la restitution des données exfiltrées et ne garantit pas la non publication de ces dernières. Enfin, le paiement incite les cybercriminels à poursuivre leurs activités, entretient ce système frauduleux et n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels. Si vous êtes une entité publique, vous pouvez utiliser les éléments suivants : « Conformément à la doctrine de l'État français et des administrations publiques, aucun paiement ne sera effectué auprès des cybercriminels. » Si votre entité décide tout de même de payer la rançon, il est obligatoire, dans le cadre du Code des assurances[6], de déposer plainte en amont afin de pouvoir activer les clauses de votre contrat d'assurance. Gardez à l'esprit que même en étant discret, un rétablissement rapide de votre système d'information mettra la puce à l'oreille des spécialistes en cybersécurité. Le paiement de la rançon ne fera pas disparaître la revendication de l'attaquant et l'information du paiement pourra même être relayée par l'attaquant.

En complément, gardez à l'esprit que :

- → **Chaque incident étant unique**, il est indispensable de réaliser des messages adaptés à la situation et aux publics identifiés ***(cf. Fiche 5).***
- → **Les messages devront évoluer tout au long de la crise**.
- → **La répétition des messages est un principe de base** de la communication et est donc à utiliser sans modération.

À RETENIR

Utilisez un ton pédagogique et rassurant pour votre communication. Évitez les termes trop anxiogènes et adaptez la technicité de l'information en fonction du public. En utilisant la méthode FACET (F pour Faits, A pour Actions, C pour Compassion, E pour Engagement et T pour Transparence), les informations communiquées doivent être factuelles et véridiques.

[6] Code des assurances, Chapitre X : L'assurance des risques de cyberattaques (Article L12-10-1).

FICHE 7 PENDANT UNE CRISE CYBER

PILOTER SA COMMUNICATION DE CRISE INTERNE

Lors d'une crise cyber, la communication interne est stratégique. Les collaborateurs doivent être informés, rassurés et alignés pour éviter les discours contradictoires, les rumeurs, les fuites d'informations voire la panique.

S'ils sont toujours disponibles, continuez d'utiliser les outils de communication interne « classiques » :

→ Réunion d'équipe ou briefing managers
(en présentiel ou en visio)

→ Email interne ou newsletter (avec un objet clair « Information importante – incident cyber en cours »), qui peut comprendre un message porté par vos dirigeants

→ Intranet

→ Réseau social d'entreprise

→ Messagerie interne

→ Solution d'affichage dynamique sur des écrans

→ Journal papier interne

→ Affichage papier dans les locaux
(salle de pause, cafétéria, etc.)

Si la crise cyber empêche l'accès à vos outils « classiques », utilisez des solutions alternatives pour maintenir la communication avec vos collaborateurs :

→ Téléphones et emails personnels

→ Application de messagerie instantanée temporaire

→ Groupe fermé sur un réseau social grand public

→ Brochure avec consignes

→ Adresse email temporaire (hors de votre système d'information) **créée sur un service de messagerie gratuit pour les particuliers**

→ Formulaire de contact sur l'intranet

→ Mode « papier crayon »

→ Courrier postal

PRIORITÉ À L'INTERNE

Il est nécessaire de donner la « primeur » de votre communication à votre cible interne (avant la communication externe) car ce sont souvent les premières personnes concernées par les impacts de l'incident. Par exemple, un rançongiciel qui bloque les accès au système d'information se manifeste souvent par l'affichage sur les écrans d'ordinateur d'une demande de rançon, voire d'un décompte. Ce mode opératoire génère très souvent émoi et anxiété au sein des équipes et empêche les collaborateurs de travailler. L'objectif est aussi d'éviter que vos collaborateurs découvrent des informations sur la crise en cours dans les médias ou sur les réseaux sociaux. Tenez également compte de leurs horaires de travail et des éventuels décalages horaires avec vos équipes à l'étranger pour définir le tempo de vos communications internes.

DISCRÉTION ET CONFIDENTIALITÉ

La porosité entre communication interne et communication externe est plus forte que jamais, ce qui implique de faire attention aux contenus diffusés aux collaborateurs ***(cf. Fiche 5)***. Il est très fréquent de voir des communications internes fuiter en externe.
La diffusion ou le rappel de la conduite à tenir de la part des collaborateurs sur les réseaux sociaux ou vis-à-vis des médias est également indispensable.

→ **Relations presse** : demandez à vos collaborateurs de ne pas répondre directement aux sollicitations des médias et de les transmettre au service de presse de votre entité ou, à défaut, aux dirigeants. L'objectif est de centraliser les échanges, d'évaluer précisément le niveau de pression médiatique et ainsi de garantir une réponse cohérente et maîtrisée.

→ **Réseaux sociaux** : il est recommandé durant la crise de restreindre les prises de parole individuelles sur l'incident en rappelant les risques réputationnels et juridiques (exemples : la clause de confidentialité du contrat de travail ou le devoir de réserve, la discrétion ou le secret professionnel pour les agents de la fonction publique).

PROXIMITÉ

Vous pouvez également utiliser l'ensemble des niveaux hiérarchiques de votre entité (managers, dirigeants, etc.) pour diffuser largement vos messages à destination de vos collaborateurs ***(cf. Fiche 5)***. En effet, le manager de proximité demeure le maillon essentiel de la chaîne d'information.

CHANGEMENT DES COMPORTEMENTS

La communication interne est un levier indispensable pour faire changer les comportements en matière de cybersécurité. En cas de cyberattaque, il est fréquent d'adresser des communications internes pour expliquer la mise en place de l'authentification multifacteur (MFA) ou inciter vos collaborateurs à changer leurs mots de passe. L'enjeu est alors d'accompagner le changement sans créer une vague de panique ou de désorganisation en interne.

« Une communication de crise maîtrisée implique d'informer rapidement et régulièrement les collaborateurs. Les modalités de communication interne doivent donc être définies à froid. Cela est d'autant plus vrai lorsqu'il s'agit d'anticiper une cyberattaque pouvant provoquer l'indisponibilité de certains outils de communication interne. »

Clémence Picart
Directrice adjointe du dialogue et de la communication de l'Autorité de sûreté nucléaire et de radioprotection

À RETENIR

Informez en priorité vos collaborateurs pour éviter rumeurs et panique. Utilisez des moyens alternatifs si vos canaux « classiques » sont indisponibles. Gardez en tête que vos communications internes risquent de fuiter en externe. Rappelez la conduite à tenir à vos collaborateurs sur les réseaux sociaux ou vis-à-vis des médias. La communication interne vous permettra également d'accompagner les collaborateurs vers de nouvelles pratiques plus sécurisées.

FICHE 8 PENDANT UNE CRISE CYBER

PILOTER SA COMMUNICATION DE CRISE EXTERNE

LA VEILLE MÉDIATIQUE

Durant une crise cyber, la veille médiatique est un outil stratégique incontournable pour concevoir et adapter la posture de communication.
En amont de la crise, le veille peut permettre de déceler des signaux faibles, notamment sur les réseaux sociaux, annonciateurs d'un incident technique (publication d'un influenceur, revendication d'un attaquant, etc.). Dans ce cas, le communicant doit alerter les différentes parties prenantes concernées (dirigeants de l'entité, équipe cyber/informatique, etc.).

Au démarrage et pendant la crise cyber, une veille couvrant les médias et les réseaux sociaux, doit être mise en place et suivie si possible par une personne dédiée. Il est également utile de suivre les éventuelles prises de parole politiques et les réactions des collaborateurs en interne (en lien avec le chargé de communication interne). Cette veille permettra de mieux comprendre la réalité médiatique et la pression subie par votre entité, d'orienter votre communication de crise cyber, d'évaluer l'efficacité de celle-ci et d'identifier les questions récurrentes ou critiques fréquentes de vos parties prenantes sur l'incident et sur sa gestion.

Face à la masse d'informations disponibles, réaliser une veille efficace nécessite une démarche méthodique.

1/ IDENTIFIEZ LES INFORMATIONS PERTINENTES SUR VOTRE INCIDENT À VEILLER

Pour suivre la perception de la situation, sélectionnez les bons mots-clés et associez-les à vos outils de veille. Ils doivent être suffisamment larges pour capter un maximum d'informations pertinentes, mais assez précis pour éviter un trop plein de « bruit médiatique ». Pensez à les décliner au pluriel et en différentes langues. Par exemple :

- → **Le nom de votre entité**
- → **Le nom des produits ou services**
- → **Le nom de vos dirigeants**
- → **Les termes** « cyberattaque », « incident », « attaque cyber », « attaque informatique », « incident de sécurité », « fuite de données », « vol de données », « vente de données », « publication de données », « piratage », « rançon », « *ransomware* », « *malware* », « faille de sécurité », « DDoS », « déni de service », « hameçonnage », « vulnérabilité », etc.

2/ IDENTIFIEZ LES SOURCES PERTINENTES À VEILLER

Sélectionnez les sources médiatiques que vous souhaitez suivre :

- → **Agences de presse**
- → **Presse écrite** (titres nationaux, régionaux, internationaux, spécialisés dans votre secteur d'activité, etc.) et leurs déclinaisons (papier, web et comptes sur les réseaux sociaux)
- → **Médias en ligne** (sites d'actualités généralistes et thématiques, blogs influents, forums de discussion, etc.)
- → **Réseaux sociaux** comprenant des comptes de journalistes, experts, leaders d'opinion et influenceurs
- → **Radios et télévisions** (locales, régionales, nationales et internationales)

3/ UTILISEZ DES OUTILS PERTINENTS DE VEILLE

Plusieurs outils et services de veille existent, gratuits ou payants :

- → **Des outils d'alerte** vous envoient des notifications directement par email lorsque des contenus récemment publiés (uniquement sur le web) contiennent vos mots-clés.
- → **Des outils automatiques** (agrégateurs de contenus ou plateformes de veille professionnelles) vous permettent de tout regrouper au même endroit et travaillent automatiquement en repérant en temps réel les contenus publiés avec vos mots-clés sur l'ensemble des sources.
- → **Des agences de communication spécialisées** peuvent également effectuer cette veille pour vous.

4/ ANALYSEZ ET DIFFUSEZ EN INTERNE LES RÉSULTATS DE VOTRE VEILLE

Une fois que vos outils ont repéré des contenus liés à vos mots-clés, analysez-les attentivement en adoptant une vision d'ensemble. Pour faciliter cette démarche, la création de tableaux de bord est recommandée (à l'aide de différents graphiques afin de visualiser rapidement les grandes tendances qui se dégagent). Durant votre crise cyber, votre veille médiatique vous permettra d'analyser :

- → **Le volume** des publications, mentions, *likes*, impressions, commentaires, repartages, etc.
- → **La tonalité des messages** : positive (soutien, engagement favorable), négative (critique, polémique, mécontentement), neutre (partage d'informations factuel).
- → **Les narratifs dominants** (reprise de vos messages clés, rumeurs, accusations, attentes de vos parties prenantes, etc.).
- → **La vitesse de propagation des informations.**
- → **Les prises de parole sur les réseaux sociaux** (des dirigeants, de vos collaborateurs, des représentants du personnel, etc.).
- → **Les sources des messages** (journalistes, influenceurs, personnel politique, etc.) mais également la diffusion par des bots de fausses informations.
- → **Le relai et l'engagement suscités par vos actions de communication de crise** (viralité du partage d'un communiqué de presse, engagement de vos publications dédiées à l'incident, etc.).

Les résultats de votre veille peuvent être partagés efficacement en interne via des rapports de veille (qui peuvent aussi être générés automatiquement par les outils), des alertes email, une newsletter, sur l'intranet, etc.

Les *chatbots* d'intelligence artificielle (IA) génératifs, très utilisés sur certains réseaux sociaux, sont devenus des leaders d'opinion et évoquent peut-être déjà votre entité. Lors d'une crise cyber, ils peuvent avancer des informations fausses ou partiellement vraies concernant votre entité, que les utilisateurs peuvent parfois prendre comme véridiques. Il est donc crucial de prendre en compte ces nouvelles sources d'informations dans votre veille médiatique.

LA COMMUNICATION DIGITALE

Les réseaux sociaux et le site web sont des outils incontournables en communication de crise cyber dont il faut faire usage à bon escient.

Suspendez toutes les communications prévues sur vos réseaux sociaux jusqu'à ce que vous ayez défini votre stratégie de communication de crise. N'oubliez pas de supprimer les publications programmées ou sponsorisées sur vos outils de *social media management*. Assurez-vous de la pertinence de votre actualité à la Une sur votre site web au moment de l'incident.

L'information (et la désinformation) circule vite sur les réseaux sociaux, et le public s'attend à des réponses immédiates. Sans précipitation, assurez-vous que **la première publication publiée sur vos réseaux sociaux après le déclenchement de la crise est une réponse pertinente** et qui résonne pour vos cibles externes. La première impression est la plus importante !

Les réseaux sociaux sont des plateformes pour diffuser des informations officielles mais également maintenir le dialogue avec le public. Il est par conséquent **nécessaire de gérer les commentaires ou publications des internautes intelligemment**. Vous pouvez répondre aux critiques légitimes avec des EDL réactifs (à adapter selon votre ligne éditoriale

habituelle) ou rediriger vers un canal privé si nécessaire. Il est conseillé de laisser visibles les commentaires négatifs pour éviter une surréaction de leurs auteurs mais déconseillé de répondre aux trolls, particulièrement présents sur certains réseaux sociaux. Leur objectif est de vous discréditer en vous poussant à la faute par tous les moyens, et le plus souvent par la malice et la provocation.

Il est préférable d'**adapter votre message à chaque plateforme en soignant le format des publications** (photo, vidéo, image, texte, etc.). Prenez la précaution de cacher les informations sensibles sur les photos et utilisez des emojis. Il est également nécessaire d'utiliser un hashtag pertinent, souvent le plus utilisé pour qualifier l'évènement en cours. Une attention particulière doit également être portée à la régularité et aux horaires des publications pour être visible par le plus grand nombre. Attention cependant à ne pas trop multiplier les formats afin de conserver une communication d'ensemble cohérente.

Ne laissez pas vos collaborateurs *(cf. Fiche 7)* alimenter la crise médiatique par des déclarations spontanées et maladroites sur les réseaux sociaux. À la place, en utilisant le cas échéant votre programme d'*employee advocacy*, il est recommandé de faire appel aux collaborateurs clés, « vos ambassadeurs », pour qu'ils puissent diffuser des informations prédéterminées et validées via leurs comptes réseaux sociaux. Votre communication sera par conséquent davantage incarnée et amplifiée.

Pour partager vos messages, vous pouvez **utiliser l'espace « Actualités » de votre site web**. Si l'incident rend votre site web indisponible, vous pouvez mettre en place un site temporaire le temps de la crise avec les informations essentielles sur votre entité. Si, faute de temps, vous ne pouvez pas l'alimenter, indiquez rapidement dans un bandeau sur votre page d'accueil que les informations concernant la crise cyber en cours sont consultables sur vos comptes réseaux sociaux.

Pour réaliser une communication transparente sur les réseaux sociaux, **montrer les coulisses de la gestion de crise peut être très utile**. Vous pouvez pour cela réaliser des publications (photos, etc.) avec vos collaborateurs « en action » lors de la mise en place de mesures permettant la continuité de service.

Gardez en tête qu'**une publication peut devenir virale et susciter beaucoup de réactions**. Cette diffusion rapide et imprévisible peut être positive, ou au contraire, se transformer en *bad buzz* atteignant ainsi l'image de votre entité ou de vos dirigeants. Le phénomène prend le plus souvent naissance sur les réseaux sociaux avant de se prolonger éventuellement sur d'autres médias.

Vous pouvez également diffuser votre conférence de presse en direct sur les réseaux sociaux pour en maximiser la portée auprès d'une large communauté, pas seulement de journalistes.

Les réseaux sociaux (et notamment LinkedIn) permettent au dirigeant de porter des messages lors d'une crise de manière simultanée et directe (sans le filtre d'intermédiaires), à différentes parties prenantes (collaborateurs, clients, usagers, investisseurs, médias, etc.). **La parole du dirigeant, en son nom, permet d'humaniser le message et de rassurer en montrant que la crise est gérée au plus haut niveau**. Les publications de votre dirigeant peuvent également être repartagées par les comptes réseaux sociaux de votre entité.

LES RELATIONS PRESSE

La manière dont vous interagissez avec les journalistes pendant une crise cyber aura un impact significatif sur la perception de vos cibles (clients/usagers, prestataires, partenaires financiers, autorités, collaborateurs, citoyens, etc.). Vous devez réussir à créer une relation de confiance avec les journalistes, basée sur le respect de leurs contraintes, la transparence et la régularité des informations transmises. Gardez à l'esprit que vous ne pouvez pas contrôler certains paramètres déterminants :

- → Chaque journaliste est libre de ses choix éditoriaux (le titre, l'angle, etc.), et il décide avec sa hiérarchie de reprendre ou non les informations transmises.
- → La priorité éditoriale peut changer à tout moment en fonction de l'actualité et vous n'avez pas la possibilité de fixer l'heure de publication.

Dans un contexte de défiance médiatique, d'infobésité, de montée en puissance de l'intelligence artificielle, les relations presse peuvent jouer, en fournissant aux journalistes des informations fiables et vérifiées, un rôle de rempart contre la désinformation.

Il est donc crucial de travailler étroitement avec votre équipe en charge des relations presse pour préparer les différents contenus à destination des journalistes :

→ **Un communiqué de presse** (voir focus dédié)
→ **Une interview** (voir focus dédié)
→ **Une conférence de presse** (voir focus dédié)

Avant toute chose, si la cyberattaque que vous subissez est visible, mettez en pause toutes les actions presse que vous aviez prévues avant le déclenchement de l'incident. La crise cyber en cours sera le seul sujet d'intérêt des journalistes, il n'est donc pas opportun de communiquer comme si de rien n'était sur d'autres thématiques.

En cas d'incident, vous pourrez être sollicité par vos contacts journalistes habituels mais également par la presse spécialisée en informatique et par les journalistes de médias généralistes travaillant au sein des services cybersécurité/tech. L'ANSSI ne communique généralement pas à la place des victimes, c'est pourquoi nous redirigeons automatiquement les demandes presse reçues sur les incidents vers les (potentielles !) victimes.

Le rôle de chacun en matière de communication de crise cyber doit clairement être défini, partagé et compris par tous. Pour une meilleure maîtrise du message, il est conseillé de limiter le nombre d'interlocuteurs des médias et de les préparer en amont à l'exercice de la prise de parole médiatique. En période de crise, le dirigeant incarne naturellement le porte-parole privilégié : sa prise de parole souligne l'engagement fort de l'entité et renforce la crédibilité des messages diffusés. Cependant, plusieurs autres porte-paroles peuvent également être identifiés et utilisés de manière graduelle, afin de mobiliser le dirigeant uniquement au plus fort de la crise.

FOCUS
L'IA, UN RECOURS PARFOIS UTILE EN TEMPS DE CRISE

À noter qu'une relecture orthographique de vos contenus avant publication est a minima une action réalisable par une IA générative. Vous pouvez également demander à une IA, à l'aide d'un prompt pertinent, d'écrire vos différents contenus de communication de crise (communiqués de presse, publications réseaux sociaux, etc.). Cependant, ne transmettez aucune données sensibles ou confidentielles à ce type d'outils et relisez avec un sens critique les contenus proposés. Le Service d'information du Gouvernement (SIG) a élaboré une charte d'usage de l'intelligence artificielle pour les communicants de l'État, en cohérence avec les autres référentiels communs (marque de l'État, charte d'accessibilité, système de design de l'État). Vous trouverez ce document sur le site *Info.gouv.fr*.

1/ LE COMMUNIQUÉ DE PRESSE

Le communiqué de presse est un outil très utile lors d'une crise cyber lorsqu'il est bien rédigé mais il peut être contre-productif s'il est trop compliqué à comprendre, s'il est trop succinct ou s'il n'est pas envoyé aux bons destinataires.

→ AVANT DE COMMENCER

Il est nécessaire de réfléchir à l'objectif que vous voulez atteindre avec la diffusion d'un communiqué de presse. Avant de le rédiger, posez-vous les questions suivantes :

POUR QUI J'ÉCRIS ?
Si vous communiquez sur une crise cyber, vous vous adresserez à la fois à des journalistes spécialisés cybersécurité/tech (et leur lectorat) et à des journalistes généralistes (et leur lectorat).

POURQUOI J'EN PARLE ?
Les journalistes reçoivent plusieurs dizaines de communiqués de presse par jour, le vôtre doit être efficace. Gardez en tête que vous n'écrivez pas pour vous, ni pour votre entité, mais pour les journalistes à qui vous vous adressez.

DE QUOI JE PARLE ?
Votre communiqué doit répondre à la règle des 6W :

▸ Who / Qui ?
Qui est concerné ?
Qui est à l'origine ?
▸ What / Quoi ?
Quel est l'évènement ?
Que s'est-il passé ?
▸ When / Quand ?
Quand cela s'est-il produit ?
Quand cela va-t-il se produire ?
▸ Where / Où ?
Où cela se passe-t-il ?
▸ Why / Pourquoi ?
Pourquoi cela arrive-t-il ?
Quelles sont les causes ou les motivations ?
▸ How / Comment ?
Comment cela s'est-il produit ?
Comment réagir ?

→ LE CONTENU DE VOTRE COMMUNIQUÉ

INTRODUCTION DU COMMUNIQUÉ

Mettez votre logo, indiquez le lieu et la date, surtout si vous pouvez être amené à en republier d'autres dans les jours suivants.

LE TITRE

C'est la partie la plus importante de votre communiqué de presse :

- Rédigez-le en dernier (une fois le contenu écrit, pour qu'il reflète le reste du communiqué).

- Il doit contenir assez d'informations pour que la personne qui le reçoit comprenne rapidement de quoi il s'agit, sous la forme : Sujet > Action > Objet de l'actualité.

- Soyez concis (pas plus de deux lignes).

Lorsque votre communiqué de presse sera repris par un média, le titre sera certainement « copié/collé » puis partagé sur les réseaux sociaux.

LE CHAPÔ / L'ACCROCHE

Répondez en une ou deux phrases aux 6W énoncés un peu plus haut.

- Faites au plus simple et au plus concret.

- Ne cherchez pas à ce stade à rentrer dans les détails.

LE CORPS DU COMMUNIQUÉ

Il est recommandé d'adopter la méthode FACET
(Faits, Actions, Compassion, Engagement et Transparence)
pour rédiger le corps de votre communiqué de presse ***(cf. Fiche 6)***.
En complément :

▸ Vérifiez que votre communiqué répond bien aux 6W.

▸ Rédigez à la troisième personne, comme un journaliste le ferait dans un article de presse.

▸ Vous pouvez inclure une citation
(de préférence des dirigeants de votre entité)
pour incarner un message important.

▸ Évitez le jargon car votre communiqué
doit être accessible à tous ***(cf. Fiche 6)***.

LA CONCLUSION

▸ Ajoutez des informations complémentaires en quelques mots sur votre entité, ce que l'on appelle plus communément le « à propos » (ou *boilerplate*).

▸ Indiquez la/les personnes à contacter pour plus d'informations (votre attaché(e) de presse ou votre agence de relations presse).

2/ LA CONFÉRENCE DE PRESSE

Ce format peut être très pertinent, car il permet en une seule prise de parole de transmettre de nombreux messages à un grand nombre de journalistes. La conférence de presse présente également un intérêt pour les journalistes qui auront l'occasion d'échanger avec un ou des porte-paroles lors de la session de questions/réponses.

Cependant, cela reste un exercice périlleux : l'entité doit être en mesure de répondre aux questions, évidemment nombreuses, des journalistes sur la crise cyber ou sur tout autre sujet d'actualité.

Lorsque vous programmez votre conférence de presse, votre première préoccupation doit être de **choisir un moment et un lieu qui s'adaptent à l'emploi du temps des journalistes tout en considérant vos propres contraintes**. Vous devez également dresser une liste des médias à inviter.

Prévoyez de prévenir au plus tôt les journalistes et d'inclure dans l'invitation une brève description de l'objectif de la conférence de presse ainsi que des détails importants tels que la date, l'heure et le lieu. Ayez à l'esprit que votre conférence de presse peut être diffusée en direct sur une chaîne de télévision ou sur le web et que son impact n'en sera que plus important.

Lors d'une crise cyber, l'objectif d'une conférence de presse est généralement de faire un point d'étape sur la situation. Elle se déroule habituellement en 3 parties :

- → **Une prise de parole descendante**, d'un ou plusieurs porte-paroles.
- → **Une session de questions/réponses** avec les journalistes présents.
- → **Des interviews du porte-parole** sous forme de micro-tendu pour les médias audiovisuels à l'issue de la conférence de presse.

Des échanges informels et complémentaires avec certains journalistes peuvent également être organisés dans la foulée.

Attention, la conférence de presse a un caractère exceptionnel. Le format, de moins en moins suivi par les journalistes, car chronophage, ne peut fonctionner que s'il est perçu comme un évènement rare, qui mérite le déplacement.

3/ L'INTERVIEW

L'interview peut être réalisée par écrit, en audio (en studio, par téléphone) ou en vidéo (en plateau, en duplex), enregistrée ou en direct. Dans ce cas, le journaliste attendra de vous :

- → Des premières ou nouvelles informations vis-à-vis de votre crise cyber.
- → Du concret avec une description des faits ***(cf. Fiche 6)*** et des chiffres.
- → Un porte-parole qui s'exprime clairement, qui est précis et utilise des formules percutantes.

À noter qu'il peut être stratégique et efficace de faire une déclaration exclusive à une agence de presse majeure, telle que l'Agence France-Presse (AFP), Associated Press (AP), Reuters ou Bloomberg, selon la nature des activités et les intérêts, français ou étrangers, de votre entité. L'agence, via une dépêche, relaiera ensuite les messages à l'ensemble des médias nationaux et internationaux. Cette méthode présente plusieurs avantages :

- → **Contrôle du récit** : en limitant les sources directes, on réduit les risques de distorsion ou de multiplication des interprétations.
- → **Gain de temps** : une seule interaction avec une agence évite de multiplier les échanges avec différents journalistes.
- → **Couverture médiatique large et homogène** : la dépêche, reprise par les rédactions, assure une diffusion rapide et unifiée de l'information.

« Victime d'une cyberattaque en 2025 atteignant ses bases de données, la ville a immédiatement informé les usagers. Habituée à la gestion de crise par son exposition aux risques industriels, la ville a appliqué les mêmes méthodes, une information précise portant sur les faits et les conséquences connues de l'attaque. »

Romain Boix
Directeur de Cabinet,
Pont-de-Claix

À RETENIR

En cas de crise cyber, la veille médiatique est indispensable : surveillez les mentions, la tonalité des échanges, et les narratifs dominants pour ajuster votre communication en temps réel. Les réseaux sociaux et le site web sont des canaux stratégiques : suspendez les publications programmées et adaptez vos messages à chaque plateforme. Pour les relations presse, centralisez les demandes via le service de presse et préparez un communiqué de presse en suivant la méthode FACET et la règle des 6W. Attendez-vous à être sollicité par vos contacts médiatiques habituels, mais aussi par des journalistes spécialisés en cybersécurité/tech. L'ANSSI ne se substitue pas aux victimes pour communiquer et redirige systématiquement les demandes presse vers l'entité concernée.

APRÈS UNE CRISE CYBER

Lorsque votre crise cyber se termine, les équipes sont tentées de reprendre rapidement le cours de leurs activités. Pour autant, cette période de transition vers une reprise normale de l'activité de votre entité est le meilleur moment pour réaliser plusieurs actions de communication. Des fiches pratiques détaillent ces actions dans les pages suivantes.

FICHE 9 APRÈS UNE CRISE CYBER

REMERCIER SES COLLABORATEURS ET RÉALISER SON RETEX

REMERCIER VOS COLLABORATEURS

Il est indispensable d'envoyer un message de remerciement à vos différentes parties prenantes externes mais également internes pour leur collaboration dans la résolution de votre crise cyber. Pour l'interne, ce message, idéalement signé des dirigeants de votre entité, soulignera l'effort collectif et permettra de remercier l'ensemble de vos collaborateurs pour leur professionnalisme et leur engagement durant l'incident. Il peut être complété par un rappel des bonnes pratiques de cybersécurité à adopter et annoncer la mise en place d'un retour d'expérience (RETEX).

RÉALISER VOTRE RETEX

Après la crise cyber, il est nécessaire de revenir sur les actions de communication réalisées, capitaliser sur ce qui a été vécu et ce qui pourrait être amélioré. Le RETEX participe à renforcer la résilience de votre équipe communication, en mettant en avant les points forts et les axes d'amélioration suite aux éventuels dysfonctionnements constatés. Il permet aussi de pérenniser certains dispositifs de communication de crise qui ont été jugés efficaces. Le RETEX doit s'organiser après la clôture de la crise cyber et ne doit pas être considéré comme un audit mais comme une action de capitalisation. Il se fait en deux temps :

→ **Un retour d'expérience « à chaud »** organisé sous forme d'entretiens ou d'ateliers de collecte de l'information.

→ **Un retour d'expérience « à froid »** permettant de présenter une synthèse des observations, des recommandations et le plan d'action associé.

À RETENIR Il est indispensable d'envoyer un message de remerciement à vos différentes parties prenantes internes et de réaliser un RETEX afin de revenir sur la communication réalisée pendant la crise cyber.

FICHE 10 APRÈS UNE CRISE CYBER

PARTAGER SON EXPÉRIENCE ET SENSIBILISER SES COLLABORATEURS

PARTAGER VOTRE EXPÉRIENCE

Un témoignage public peut éclairer et inspirer d'autres acteurs sur les risques et les mesures à mettre en œuvre pour prévenir les cyberattaques. En partageant votre expérience, vous illustrez concrètement comment vous avez relevé ce défi et vous contribuez à renforcer la cybersécurité dans votre secteur d'activité ou d'intervention. En complément, une crise cyber bien gérée peut être prise en exemple. Cela permettra de prouver également que votre entité sait tirer les leçons des difficultés et placer la sécurité au cœur de ses priorités.

« Durant et après la crise cyber, nous avons décidé de partager notre expérience également avec l'ensemble de notre écosystème pour mettre nos confrères en vigilance sur ce type d'attaque (*password spraying*) et leur permettre de s'en prémunir. »

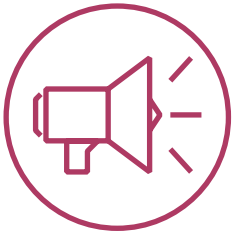
Nadèje Aroumougom
Directrice stratégie, marketing et communication, Alptis Assurances

SENSIBILISER VOS COLLABORATEURS

Une crise cyber est une opportunité, une fois sous contrôle, de remobiliser les équipes sur la cybersécurité. Ce peut être l'occasion de préparer, en lien avec l'équipe cyber/informatique, une campagne de sensibilisation en interne sur les bonnes pratiques informatiques à adopter. Selon les caractéristiques de votre entité (taille, effectif, sensibilité de l'activité, niveau de connaissance des collaborateurs, moyens de communication disponibles, etc.), des opérations de différentes natures peuvent être envisagées :

- → **Réunions d'information**
- → **Campagnes d'affichage**
- → **Distribution de guides de bonnes pratiques**
- → **Quiz**
- → **Campagne test de *phishing***

Le site ***Cybermalveillance.gouv.fr*** peut vous permettre de trouver des ressources et des idées pour mener à bien vos campagnes internes de sensibilisation.



À RETENIR Un témoignage public peut éclairer et inspirer d'autres acteurs sur les risques et les mesures à mettre en œuvre pour prévenir les cyberattaques. Une crise cyber est aussi l'occasion de remobiliser vos collaborateurs sur les bonnes pratiques informatiques à adopter.

CHECKLIST

AVANT UNE CRISE CYBER

- ◯ Initier une rencontre entre votre équipe communication et les équipes cyber/informatique afin d'avoir une meilleure compréhension mutuelle des priorités, des enjeux et du vocabulaire de chacun.
- ◯ Préparer différentes stratégies de communication sur la base des scénarios de crise cyber probables (DDoS, rançongiciel, défiguration, etc.).
- ◯ Constituer une boîte à outils dédiée à la communication de crise cyber.
- ◯ Participer à un exercice de crise cyber afin de tester la résilience de votre équipe communication et de vos outils face à une cyberattaque.
- ◯ Réaliser un *media training* de vos porte-paroles pour développer leurs réflexes.

PENDANT UNE CRISE CYBER

- ◯ Mettre en place une organisation spécifique de crise de votre équipe communication avec une répartition des rôles (coordination, perception et réaction) et des missions.
- ◯ Réaliser un état des lieux des faits, de la situation en matière de communication et du contexte.
- ◯ Proposer à vos dirigeants une posture de communication à adopter : proactive ou réactive.
- ◯ Définir vos objectifs de communication principaux (expliquer, informer, rassurer, préserver l'image et la réputation de l'entité et faire changer les comportements).
- ◯ Définir et adresser vos différentes cibles internes (collaborateurs, managers, représentants du personnel, etc.) et externes (journalistes, usagers, clients, actionnaires, partenaires, autorités, etc.).
- ◯ En cas de communication réactive, questionner le moment et la pertinence d'une première communication.

PENDANT UNE CRISE CYBER

- ◯ En cas de communication proactive, communiquer rapidement uniquement des informations vérifiées, ne pas s'engager sur une date de retour à la normale précise, informer régulièrement et occuper l'espace médiatique si cela est possible.
- ◯ Prioriser les communications en fonction de vos cibles et notamment informer en premier lieu vos collaborateurs et vos clients/usagers.
- ◯ Utiliser un ton pédagogique et rassurant.
- ◯ Éviter les termes trop anxiogènes et adapter la technicité de l'information en fonction du public.
- ◯ Communiquer des informations factuelles et véridiques.
- ◯ Utiliser des moyens alternatifs pour la communication interne si vos canaux « classiques » sont indisponibles.
- ◯ Garder également en tête que vos communications internes risquent de fuiter en externe et rappeler la conduite à tenir à vos collaborateurs sur les réseaux sociaux ou vis-à-vis des médias.
- ◯ Surveiller les mentions, la tonalité des échanges, et les narratifs dominants sur les réseaux sociaux et dans les médias pour ajuster votre communication en temps réel.
- ◯ Geler les publications programmées sur vos réseaux sociaux et adapter vos messages à chaque plateforme.
- ◯ Centraliser les demandes presse via le service de presse et préparer un communiqué de presse en suivant la méthode FACET et la règle des 6W.

APRÈS UNE CRISE CYBER

- ◯ Envoyer un message de remerciement à vos différentes parties prenantes internes.
- ◯ Réaliser un RETEX sur la communication réalisée pendant la crise cyber.
- ◯ Partager un témoignage public pour éclairer et inspirer d'autres acteurs sur les risques et les mesures à mettre en œuvre pour prévenir les cyberattaques.
- ◯ Sensibiliser vos collaborateurs sur les bonnes pratiques informatiques à adopter.

RESSOURCES

RETROUVEZ TOUS LES GUIDES DE BONNES PRATIQUES DE L'ANSSI SUR
messervices.cyber.gouv.fr

Collection Remédiation

Autres guides de la collection Crise Cyber

Rapports sur les menaces et incidents

Panoramas de la cybermenace annuels

Retrouvez également les bulletins d'actualité, les alertes et les avis de sécurité, les fiches réflexes ou encore les états de la menace informatique sectorielle du CERT-FR sur ***www.cert.ssi.gouv.fr***

CyberDico

Le CyberDico de l'ANSSI liste, par ordre alphabétique, des mots, expressions et sigles du domaine de la cybersécurité. Il présente leur traduction ainsi que leur définition en français.
www.cyber.gouv.fr/cyberdico

Version 2.0 – Juin 2026

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51 boulevard de la Tour-Maubourg — 75700 PARIS 07 SP
www.cyber.gouv.fr