RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION
GESTION DE CRISE CYBER

CRISE D'ORIGINE CYBER

LES CLÉS D'UNE GESTION OPÉRATIONNELLE ET STRATÉGIQUE

CDSE
CLUB DES **DIRECTEURS** DE **SÉCURITÉ** DES ENTREPRISES

COLLECTION
GESTION DE CRISE CYBER

GUIDE

CRISE D'ORIGINE CYBER

LES CLÉS D'UNE GESTION OPÉRATIONNELLE ET STRATÉGIQUE

SOMMAIRE

ÉDITORIAL

Commençons par une pointe de provocation. Je pourrais dire qu'il y a deux types d'organisations : celles qui ont déjà été victimes d'une cyberattaque et celles qui ne tarderont sans doute pas à l'être. Ces dernières années, de nombreuses organisations ont investi massivement dans la protection et la défense de leurs systèmes d'information et de leurs services numériques. Le risque cyber est ainsi de mieux en mieux considéré. C'est une excellente chose pour notre sécurité collective !

Mais pour assurer leur résilience, les organisations doivent se dire que ces efforts ne suffisent pas toujours… Et bel et bien se préparer à la possibilité d'une attaque. Aujourd'hui, le vol de données, la paralysie partielle ou totale des services numériques ont des impacts opérationnels, juridiques, financiers ou réputationnels critiques. On ne peut pas improviser des réponses en plein milieu d'une catastrophe ! La préparation, l'outillage et l'entraînement sont indispensables pour maintenir l'activité en cas d'attaque informatique. Et pas seulement au niveau des experts cyber, mais bien de façon transverse au sein de l'organisation en associant les directions métier, les dirigeants et les employés.

Ce guide, fruit de l'expérience d'agents de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et des membres du Club des directeurs de sécurité et de sûreté des entreprises (CDSE), vous aidera à faire de la gestion de crise cyber un véritable pilier de votre stratégie de résilience.

J'achève mon propos avec des remerciements pour Bouygues Construction, l'Hôpital Nord-Ouest de Villefranche-sur-Saône et CMA CGM. Victimes de cyberattaques, ces organisations nous ont partagé leur expérience pour illustrer les recommandations de cette publication et permettre à ses lecteurs d'appréhender concrètement la gestion de crise cyber. Merci de nous avoir offert ces précieux témoignages !

Guillaume Poupard
Directeur général de l'ANSSI

Se préparer et réagir efficacement… Cette approche présentée dans ce guide pourrait être l'un des leitmotivs du CDSE. Il est vrai que la menace cyber s'est intensifiée, avec des attaques plus nombreuses, plus sophistiquées, plus redoutables. Il est aussi vrai que la cybersécurité n'est pas toujours la priorité des organisations, alors qu'il est indispensable de toujours rester en alerte et d'y consacrer des moyens importants. Mais, dans cet océan de doutes et de vulnérabilités, il existe au moins une certitude : la diffusion de bonnes pratiques, relayées par les directeurs de la sécurité-sûreté et les experts de la sécurité des systèmes d'information des entreprises, permet d'anticiper la propagation d'un virus informatique avec plus de calme et de sérénité.

Sur le plan de la souveraineté numérique française et européenne, les prestataires de services et les fournisseurs de solutions numériques prennent aujourd'hui conscience que l'heure est venue de passer à l'action. Ils savent désormais que le prix, les fonctionnalités et l'ergonomie de leurs solutions doivent être au niveau de leurs concurrents étrangers. On peut donc se réjouir que les champions nationaux du numérique, les PME et les startups françaises constituent désormais un grand « tous ensemble cyber », qui gagnera ses parts de marché seulement s'il est performant et compétitif.

Face à l'adversité et à la croissance exponentielle de la menace cyber, il nous faut nous doter d'un bouclier protecteur et nous bâtir une sécurité numérique robuste. Les recommandations émises dans ce guide s'inscrivent dans une stratégie d'anticipation plus globale qui permettra la mise en place de cette protection.

Pour se préparer et réagir efficacement, la lecture de ce guide est donc de salubrité publique !

Stéphane Volant
Président du CDSE

INTRODUCTION

Présentation du guide

À quoi sert-il ?

Face au caractère déstabilisateur des crises d'origine cyber, ce guide a pour objectif de partager les bonnes pratiques et les recommandations utiles à toute organisation, pour d'une part, bien se préparer et d'autre part, gérer la crise étape par étape. Ces recommandations s'inspirent de retours d'expérience d'organisations, publiques comme privées, ayant été ciblées par une cyberattaque et qui ont partagé avec l'ANSSI les difficultés et succès de leur gestion de crise.

La gestion d'une crise cyber implique nécessairement des préoccupations techniques, incluant les volets cyber et technologique permettant le retour à un état de sécurité optimal, mais aussi des préoccupations plus stratégiques, incluant notamment le maintien de l'activité des métiers affectés par la crise. Pour permettre aux parties prenantes d'appréhender ces différentes préoccupations et de faciliter la prise de décision, ce guide propose des conseils pour chaque approche.

À qui s'adresse-t-il ?

Ces recommandations sont destinées à des fonctions spécifiques mais complémentaires dans le processus décisionnel de la gestion d'une crise cyber : dirigeants, responsables de la sécurité, gestionnaires des risques, responsables de la continuité d'activité ou de la gestion de crise, responsables du numérique, de la sécurité des systèmes d'information, directions métiers, fonctionnaires de sécurité et de défense, toute autre personne amenée à être mobilisée dans le cadre d'une gestion de crise cyber.

Quels sont les prérequis pour l'utiliser ?

Ce guide s'appuie sur l'hypothèse que l'organisation s'est préalablement dotée d'un dispositif global de maîtrise du risque numérique incluant les volets de gouvernance, de protection et de défense de ses systèmes d'information - ou SI - (ségrégation des réseaux, solutions de cybersécurité, sauvegardes déconnectées, outils de détection et de protection, équipes techniques dédiées, etc.) lui permettant de disposer d'un socle de sécurité résistant et adapté aux risques cyber pesant sur ses activités. Il admet également qu'il existe au sein de l'organisation un dispositif général de gestion de crise et des outils dédiés à la gestion des impacts[1] (moyens d'alerte, salle de crise, dispositif opérationnel et décisionnel, outils de conduite, plan de continuité et de reprise d'activité, etc.) contribuant à la résilience de l'organisation.

Le *Guide d'hygiène informatique* et le guide *Maîtrise du risque numérique* proposés par l'ANSSI constituent des références pour la sécurisation des SI et leur résilience[2].

Comment l'utiliser ?

Ce guide propose d'adapter des outils et des dispositifs de gestion de crise au scénario cyber. Les recommandations présentées peuvent être dissociées en fonction des volets impliqués (volets « stratégique » et « opérationnel cyber et IT »), dans la mesure où leurs objectifs de gestion de crise sont différents. Il se concentre sur des éléments jugés essentiels à la réponse de crise et n'a pas vocation à être exhaustif.

1. La famille des normes AFNOR autour de la résilience sociétale et plus particulièrement la norme ISO 22301:2019 sur le management de la continuité d'activité et la norme ISO 22320:2018 sur le management des incidents constituent des références pour la définition de ce dispositif de crise.
2. www.ssi.gouv.fr/guide/guide-dhygiene-informatique/ et www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/

Les enjeux de la préparation à la gestion d'une crise d'origine cyber

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 organisation (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[3] (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'organisation. Par convention, on parlera par la suite de « crise cyber ».

Les événements accidentels, c'est-à-dire ne résultant pas d'une activité malveillante sur les SI, et les actions malveillantes n'entraînant pas l'interruption immédiate et majeure des services essentiels de l'organisation sont par conséquent exclus du périmètre de définition. Néanmoins, les recommandations du guide peuvent être utilisées comme bonnes pratiques pour faire face à ces situations.

Les spécificités des crises cyber

En comparaison à d'autres scénarios de crise, les crises cyber ont des caractéristiques propres qu'il est important d'appréhender :

- une double temporalité, avec des impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs semaines, voire plusieurs mois ;
- une absence d'unicité de lieu de réalisation, qui sous-entend une potentielle propagation à d'autres organisations en raison de l'interconnexion des SI ;

3. Auxquels sont associés les systèmes d'information de l'organisation et ceux de ses prestataires.

- une menace s'adaptant aux mesures d'endiguement et de remédiation ;
- une incertitude concernant le périmètre de la compromission ;
- une complexité pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque.

L'acculturation des équipes décisionnelles aux questions cyber doit faciliter à la fois la bonne compréhension des implications concrètes de la crise cyber sur l'activité de l'entité et l'intégration du volet opérationnel au dispositif de crise.

« Les premières alertes ont été remontées par les pays étrangers très tôt le matin. Lorsque nous avons perdu la supervision centrale, nous avons décidé de couper le SI à l'échelle mondiale ! Une cellule de crise *ad hoc* a été mobilisée et plusieurs centaines de personnes étaient impliquées directement dans la résolution de l'incident. »

Bouygues Construction

« L'alerte a rapidement été donnée par l'astreinte informatique et nous a permis de nous rendre au datacenter pour couper les SI et stopper la propagation de l'attaque. Par la suite, les médecins ont dû reprendre un mode de gestion totalement papier pour assurer le suivi des patients. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

« Dès les premières alertes remontées par nos équipes en Asie, nous avons déclenché notre plan de réponse à incident et créé une cellule de crise. La décision de couper le SI a rapidement été prise pour stopper la propagation, déterminer l'impact et démarrer les investigations. Les équipes cyber, IT et métiers se sont mobilisées pour rapidement redonner accès aux fonctions essentielles du groupe. »

CMA CGM

PARTIE 1

SE PRÉPARER À AFFRONTER UNE CRISE CYBER

Les déséquilibres qu'implique une crise cyber forcent les organisations à s'adapter et à fonctionner de manière inhabituelle. Ces bouleversements soudains et à l'échéance incertaine sont une source de stress et compliquent la prise de décision, alors même que des actions de remédiation doivent être décidées et exécutées rapidement pour limiter les impacts.

Une gestion de crise nécessite donc une bonne préparation via la mise en place de processus et d'outils éprouvés. L'objectif est de gagner en fluidité et d'adopter des automatismes qui permettront de réagir efficacement sur le temps long et de redonner confiance aux équipes et à l'écosystème concernés directement ou indirectement par les conséquences de l'incident.

Cette première partie a pour but d'aider les entités à construire une organisation de crise résiliente, permettant de limiter les impacts de la crise cyber, de maintenir la confiance de l'écosystème, de prioriser et de conserver en mode dégradé les activités critiques affectées. Plus concrètement, il propose des conseils pratiques pour adapter les dispositifs et les outils de gestion de crise (cellule de gestion de crise, moyens logistiques dédiés, plans de réaction et de continuité d'activité, etc.) aux spécificités des impacts de la crise cyber.

FICHE 1
CONNAÎTRE ET MAÎTRISER SES SYSTÈMES D'INFORMATION

L'enjeu premier de toute équipe de gestion de crise est de pouvoir évaluer l'étendue des impacts de l'évènement sur le périmètre de l'organisation.

Dans le cadre d'une crise cyber, il est ainsi essentiel de pouvoir identifier et caractériser le périmètre de compromission, soit le chemin pris par l'attaquant pour s'introduire et se propager dans les SI, ainsi que l'impact d'une attaque sur les services numériques et la continuité des activités métiers de l'entité. Au minimum, il est conseillé de disposer des éléments suivants pour permettre aux équipes techniques (cyber et IT) de réaliser ces investigations[4] :

- une liste des applications et des services critiques rendus par l'organisation ;
- une cartographie des systèmes sur lesquels les services métiers critiques reposent et sont reliés entre eux ;
- une cartographie des périphériques des SI ;
- une liste des interdépendances des SI entre les métiers et les partenaires extérieurs (partenaires, sous-traitants, infogérants, etc.) ;
- une cartographie des parties prenantes avec les points de contact (en particulier si une partie des SI est en sous-traitance)[5] ;
- une liste des moyens de supervision et de détection et leur périmètre ;
- une politique de rétention des journaux/logs applicatifs et réseaux ;
- une matrice des flux d'information ;
- les architectures des réseaux et des éléments fonctionnels, permettant de faire le lien entre les SI et les processus métiers.

4. L'utilisation du guide *Cartographie du système d'information* est préconisée pour cette action : www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf
5. L'utilisation de l'atelier 3 de la méthode Ebios Risk Manager est préconisée pour cette action : www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Cartographier ses applications et ressources métiers critiques**	**Cartographier ses SI**
RECOMMANDATIONS	Une cartographie des services, des applications et des activités critiques, ainsi que des données essentielles est à jour et sauvegardée hors-ligne pour d'identifier les **actifs** à protéger et à surveiller en priorité et/ou à relancer en cas de crise. **Le bilan d'impact sur l'activité** peut être utilisé pour faciliter l'identification des ressources critiques de l'organisation. Une liste des services critiques et des applications associées est au minimum disponible hors ligne.	Une cartographie des principaux actifs technologiques et leurs dépendances est à jour et sauvegardée hors ligne pour faciliter les investigations numériques. En cas d'externalisation de tout ou partie des services numériques, une cartographie avec les interconnexions est à jour et disponible hors ligne. Des contacts d'urgence des prestataires sont disponibles hors ligne.

« Il est indispensable d'avoir une vision à jour des actifs numériques, dont ceux liés aux activités critiques ou hébergeant des données sensibles ou réglementées. Cela permet de prioriser les actions quand on ne peut pas tout sauver ou isoler. Il est aussi important de savoir quels collaborateurs gèrent quels systèmes, car ils sont souvent les seuls à pouvoir intervenir avec précision. Enfin, connaître ses clients et ses partenaires permet de communiquer avec eux en cas de panne ou de problème de sécurité. »

CMA CGM

FICHE 2

METTRE EN PLACE UN SOCLE DE CAPACITÉS OPÉRATIONNELLES GARANTISSANT UN NIVEAU ADAPTÉ DE RÉSILIENCE NUMÉRIQUE

Une organisation est jugée résiliente si, en cas de crise cyber, elle est capable de maintenir ses activités les plus critiques (éventuellement en mode dégradé, voire sans services et outils numériques disponibles) et de les relancer de façon maîtrisée afin de limiter les impacts de l'attaque sur son organisation, son secteur d'activité et ses clients et ainsi maintenir la confiance de l'écosystème.

Pour cela, il est important qu'elle ait mis en place des méthodes et des moyens opérationnels adaptés aux scénarios de crise cyber, qui seront mobilisés pour maintenir ou rétablir ses activités critiques. Un important travail de pédagogie devra être mené par les équipes cyber et IT auprès des métiers afin qu'ils prennent en compte les impacts cyber et adaptent leurs pratiques et leurs processus de travail (notamment le maintien de leurs activités sans services et outils numériques).

La prise en compte de **scénarios cyber de référence**, identifiés grâce à une analyse des risques stratégiques[6], permet d'adapter ces pratiques ainsi que le dispositif de gestion de crise.

6. L'utilisation de l'atelier 3 de la méthode EBIOS Risk Manager est préconisée pour cette action : www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Adapter le plan de continuité d'activité au scénario de crise cyber** **Le plan de continuité d'activité (PCA)** intervient surtout pour des scénarios uniques d'indisponibilité des ressources clés (humaines, SI, systèmes industriels, prestataires ou bâtiments). Dans le cas d'une crise cyber, le PCA doit prendre en compte l'indisponibilité de plusieurs ressources simultanées, voire une activité sans services et sans outils numériques (serveurs chiffrés, arrêt total des systèmes afin d'éviter la propagation de l'attaque, etc.).	
RECOMMANDATIONS	Le PCA inclut l'analyse, l'évaluation et le traitement des risques numériques et cyber et prend notamment en compte une perte totale ou un fonctionnement très dégradé des services et des processus critiques de l'organisation. Des solutions de continuité d'activité sont envisagées en lien avec les équipes cyber et IT. Des mesures relatives au PCA, tel que le **temps d'arrêt maximal tolérable** et le **temps de récupération des données** sont définies en intégrant les scénarios cyber. À noter que les impacts d'une crise cyber peuvent parfois fausser les mesures définies en amont. Des dispositifs opérationnels métiers sont envisagés et maintiennent à un seuil minimum le fonctionnement des processus critiques de l'organisation. Les périmètres du PCA intègrent également la perte d'une solution nuagique, d'un partenaire ou prestataire de l'entité. Les modalités de gestion de crise cyber sont intégrées dans les contrats d'infogérance et d'externalisation.	Les équipes cyber et IT accompagnent les métiers pour l'analyse, l'évaluation et le traitement des risques numériques et cyber via un travail de pédagogie et une compréhension des impacts pour l'activité métiers. Un plan de sauvegarde et de restauration des données est défini, avec des procédures de basculement sur un réseau de secours résistant aux cyberattaques. Il s'appuie sur l'existence de **sauvegardes saines**. Ces dernières sont cataloguées dans un stockage protégé. Le risque d'une incohérence de données liées à leur synchronisation est pris en compte. En cas d'indisponibilité des services et outils numériques, des solutions de continuité d'activité[7] sont définies, testées et mises à jour. L'état de la menace cyber[8] est régulièrement revu et alimente la réflexion sur la résilience des solutions et des processus mis en place.

7. De préférence qualifiées par l'ANSSI : www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/
8. Les alertes et rapports du CERT-FR constituent des sources fiables et détaillées à ce sujet : www.cert.ssi.gouv.fr/

OBJECTIF 2	**Réaliser un plan de reprise d'activité pour le scénario cyber** Construit en complément du PCA, **le plan de reprise d'activité (PRA)** assure la reconstruction de l'infrastructure numérique et la remise en route des applications stratégiques d'une organisation en cas de sinistre. Dans le cas d'une crise cyber, le PRA doit prendre en compte l'indisponibilité partielle ou totale des infrastructures numériques et la priorisation des actions de remédiation.	
RECOMMANDATIONS	Les métiers définissent pour chaque service la durée **maximum d'interruption d'activité** intégrant un temps d'indisponibilité long, lié au scénario cyber.	• Un planning des actions prioritaires pour relancer les services numériques et rétablir l'activité des métiers en cas de crise est formalisé. • En particulier, les reconstructions de l'**Active Directory**, des serveurs, des postes de travail, des **systèmes de noms de domaines** (DNS), des **infrastructures de gestion des clés (PKI), ou toute infrastructure critique,** sont prévues pour rétablir les services dans un délai acceptable. • Des procédures de basculement sur un réseau de secours sont formalisées et testées. • Des processus de restauration des données et de réinstallation des SI sont formalisés et testés.

« Un plan de réponse à incident formalisé, associé à des scénarios de menaces, sert de référence aux équipes pour aligner et concerter leurs actions de façon à sauver un temps précieux tout au long de la crise. Il formalise les dispositifs et les processus afin que les actions soient considérées dans le bon ordre et que des questions pertinentes soient soulevées assez tôt. Il inclut également des outils et des procédures, ainsi que les rôles et les responsabilités de chacun. »

CMA CGM

OBJECTIF 3	**Mettre en place des outils de conduite de crise résilients** L'indisponibilité partielle ou totale des services et des outils numériques rend difficile toute communication entre les différentes entités de l'organisation. Les cellules de crise doivent dès lors disposer d'outils « de secours » pour assurer, au minimum, le fonctionnement du dispositif de crise.	
RECOMMANDATIONS	• Des procédures de gestion de crise cyber sont mises en place et stockées hors ligne. • Un annuaire de crise des parties prenantes internes et externes (dont les contacts hiérarchiques, géographiques, infogérants, fournisseurs, autorités) est stocké hors ligne. • Des outils numériques dédiés à la cellule de crise sont prévus pour être accessibles hors ligne. Ils sont maintenus en conditions opérationnelles. • Des moyens de communication alternatifs[9] internes et externes sont identifiés et testés.	• Des procédures de gestion de crise sont mises en place et stockées hors ligne. • Un annuaire de crise des parties prenantes internes et externes est stocké hors ligne. • Des outils numériques déconnectés, dédiés à la cellule de crise, en particulier pour réaliser les investigations numériques, sont mis en place. • Des moyens de communication alternatifs[10] internes et externes sont identifiés et testés.

« Des canaux de communication alternatifs doivent être mis en place lorsque les systèmes de communication nominaux (téléphonie, mails) ne sont plus opérationnels. L'existence d'annuaires de crise déconnectés du SI est indispensable pour ajouter rapidement les parties-prenantes aux boucles d'information. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

9. De préférence qualifiés par l'ANSSI : www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/
10. *Ibid.*

FICHE 3

FORMALISER UNE STRATÉGIE DE COMMUNICATION DE CRISE CYBER

Une organisation touchée par une crise cyber peut, en fonction de son ampleur, être rapidement confrontée à des pressions internes et externes (médias, clients, partenaires) susceptibles d'affecter sa réputation.

D'une part, il est donc important que la communication soit intégrée au dispositif de gestion de crise pour accompagner les équipes lorsqu'elles alertent et conseillent les parties prenantes (clients, fournisseurs, médias, autorités, etc.) dans les meilleurs délais et pour préserver la réputation (médiatique, financière, juridique, etc.) et la confiance dans l'organisation.

D'autre part, il est nécessaire de préparer en amont de toute crise des outils et des procédures pour pouvoir anticiper les réactions, les interrogations et les perceptions de l'ensemble des parties prenantes, ainsi que de communiquer de la manière la plus appropriée sur un sujet technique.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Établir une liste des parties prenantes à contacter**	
RECOMMANDATIONS	Une liste des parties prenantes à alerter[11] (partenaires, autorités, clients, etc.) est pré-identifiée avec les contacts et les canaux de communication de secours devant être utilisés. Un contact d'urgence est identifié dans les contrats avec les clients et les fournisseurs les plus critiques. Un fichier presse est disponible et stocké hors ligne.	Une contribution sur la cartographie des parties prenantes à alerter est envisagée.

11. En fonction de la législation en vigueur et du statut de l'organisation : www.ssi.gouv.fr/en-cas-dincident/

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 2	**Anticiper la stratégie de communication de crise**	
RECOMMANDATIONS	Une stratégie de communication et un plan de communication cyber sont formalisés et validés pour maintenir la confiance, faciliter la définition de la posture de communication et l'organisation des équipes pendant la conduite de crise. Des messages types sont formalisés en fonction des scénarios cyber de référence identifiés, afin de servir d'éléments de réponse clés en main et de gagner du temps. Des équipes sont familiarisées et entraînées à la communication de crise cyber et assurent une formation régulière auprès des agents et des responsables de l'entité.	Une première analyse de risque médiatique s'appuie sur les scénarios de référence cyber. Cette analyse facilite la construction d'éléments de langage en lien avec les métiers techniques. Plusieurs sujets médiatiques spécifiques au cyber sont à anticiper (e.g. attribution de l'attaque). Le contenu des messages est revu avec les équipes communication afin de vérifier la crédibilité des éléments techniques formalisés. Des canaux de communication utilisables en cas de crise, y compris en cas d'indisponibilité des outils classiques (mails) sont identifiés pour atteindre les différentes cibles.

« Nous avons immédiatement intégré la direction de la communication dans la cellule de crise. Ils ont pu être présents dès les premières heures et avoir accès à l'information directement. Ils ont ainsi vu et compris ce qu'il se passait et ont pu établir une stratégie de communication répondant à toutes les sollicitations internes et externes. »

Bouygues Construction

FICHE 4

ADAPTER SON ORGANISATION DE CRISE AU SCÉNARIO CYBER

La particularité du scénario de crise cyber implique de mobiliser à la fois des profils métiers, cyber et IT, ainsi que d'assurer la bonne coordination entre les différents niveaux. Il convient donc de planifier une organisation de crise en amont de tout événement et de s'accorder sur le rôle de chaque partie, afin de faciliter la mobilisation.

Le dispositif de crise à établir se compose d'un volet stratégique, porté au minimum par une cellule de crise dite « stratégique » ou « décisionnelle ». Elle regroupe les représentants des fonctions décisionnelles de l'entité, qui s'approprient les fonctions usuelles d'une cellule de crise : directeur de crise, personnes en charge du management de l'information, appui à la conduite de crise, communicants, etc.

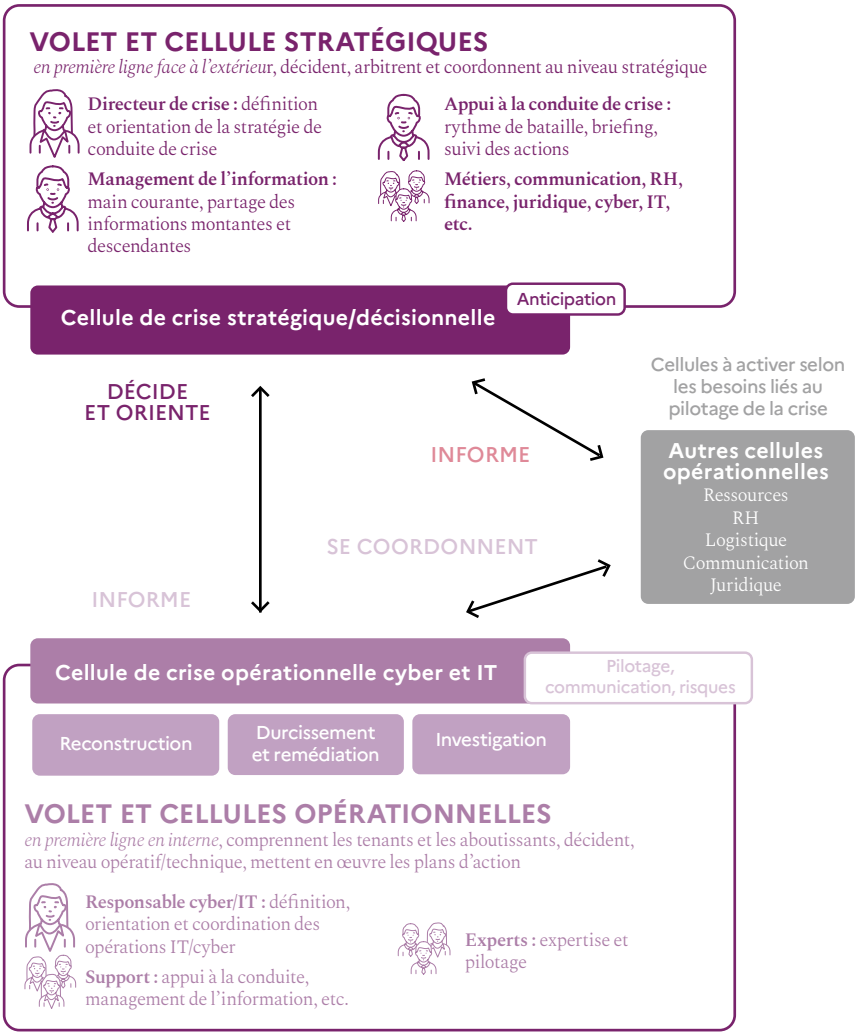
Un volet opérationnel est également mis en place. Au sein de l'organisation, les fonctions cyber et IT sont en charge du pilotage d'une ou de plusieurs cellules et s'assurent d'échanger avec la cellule stratégique.

En fonction des impacts de la crise à gérer, d'autres cellules peuvent également être mises en place : cellules métiers, cellule communication, cellule RH, cellule logistique, cellule juridique, cellule de crise opérationnelle cyber et IT, etc.

« Nous avons mis en place une organisation agile autour du duo formé par notre DGA et le DSI et de "task forces", qui nous a permis d'être réactif en fonction des urgences. Une "cellule ressource" était chargée de rassembler des prestataires et des renforts et d'aider nos équipes à se focaliser sur leur cœur de métier. »

Bouygues Construction

PROPOSITION D'ORGANISATION DE GESTION DE CRISE CYBER[12]



12. À noter que cette organisation est particulièrement adaptée aux grands groupes. Toutefois, elle peut également s'appliquer aux plus petites entités.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Mettre en place des critères et des procédures d'activation des cellules de crise**	
RECOMMANDATIONS	Les critères d'activation et de désactivation sont établis en fonction des scénarios de référence cyber définis et permettent d'objectiver la mobilisation et la démobilisation d'une cellule stratégique. Ils sont connus des membres du dispositif. Une chaîne d'alerte est formalisée. Plusieurs modes sont prévus dont un mode « alerte » et un mode « crise ». Un référentiel de management des crises cyber intégrant une description de l'ensemble du dispositif de crise (organisation, gouvernance, ressources, outils, annuaire) est formalisé, promu et maintenu à jour. Les fonctions décisionnelles de l'organisation sont sensibilisées aux enjeux cyber. Les fonctions cyber et IT sont systématiquement représentées dans la gouvernance de crise (cyber et hors cyber).	Un processus d'alerte, de gestion et de réponse aux incidents intégrant un volet « sécurité du numérique » est formalisé et testé. Il s'appuie notamment sur des outils de détection et de gestion d'incident[13]. Les critères d'activation et de désactivation du dispositif opérationnel sont définis en fonction des scénarios cyber de référence. Ils prévoient en particulier l'activation par effet de seuil (par le bas) et l'activation sur décision du dispositif stratégique (par le haut). Ils sont connus des membres du dispositif de crise et des équipes de gestion d'incident. Une chaîne d'alerte est formalisée. Plusieurs modes sont prévus dont un mode « alerte » et un mode « crise ».

13. Les outils de détection et de gestion d'incident qualifiés par l'ANSSI attestent d'une conformité à des exigences règlementaires, techniques et de sécurité : www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/

OBJECTIF 2	Organiser ses cellules de crise cyber	
RECOMMANDATIONS	Une fois les membres de la cellule de crise identifiés, ils sont informés de leur nomination au dispositif, de leur rôle et de leurs missions et y sont formés. Le périmètre d'action de chaque membre (rôles et responsabilités) est défini en amont. Une interface unique (type tableau de bord) est mise en place pour uniformiser la circulation de l'information. Des objectifs et des critères de sortie de crise atteignables sont pré-identifiés. Selon le niveau de maturité de l'organisation, un volet d'anticipation peut être mis en place pour identifier les scénarios de dégradation ou d'amélioration de la situation. Selon le périmètre géographique de l'entité, les problématiques internationales sont prises en compte (différences liées aux fuseaux horaires, aux systèmes pénaux, aux cultures, etc.) et des relais sont identifiés.	Une organisation de crise similaire à la cellule de crise stratégique est définie. Elle intègre des experts clés capables de fournir des orientations ainsi qu'un relais pour la communication de crise. L'organisation de crise en place doit être la plus efficace possible et ne s'appuie pas forcément sur l'organisation usuelle interne. Les équipes techniques cyber et IT sont organisées de manière à réaliser les actions d'investigation/endiguement, de durcissement/remédiation et de reconstruction. Un registre est mis en place pour suivre les risques, les dérogations, et les communications internes et externes.

FICHE 5
PRÉPARER SES CAPACITÉS DE RÉPONSE À INCIDENT

Idéalement, chaque organisation devrait être dotée d'une cellule de réponse à incident (CERT ou CSIRT).

Autrement, il est au minimum recommandé de mettre en place des outils de détection et de réponse à incident et de s'entourer d'experts et de prestataires[14] pour accompagner les équipes métiers et cyber dans le renforcement de leurs capacités de détection, d'investigation et de gestion des impacts de la crise.

Un travail de ciblage ou de pré-contractualisation peut être effectué en amont (via des contrats-cadres ou des référencements), en prenant en compte les compétences déjà représentées au sein de l'organisation. À noter que la souscription à une assurance cyber adaptée aux besoins de l'organisation permet également la mise à disposition de capacités et d'expertises en cas de crise.

Il est important que les prestataires identifiés soient connus par l'ensemble des acteurs de la gestion de crise, afin qu'ils puissent solliciter rapidement leur expertise. Cette liste doit régulièrement être mise à jour.

« Il faut penser à mobiliser des experts d'autres entités et accepter de ne pas tout faire en même temps, pour positionner les équipes au bon endroit. »

Bouygues Construction

14. De préférence qualifiés par l'ANSSI : www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Identifier les experts à solliciter en temps de crise**	
RECOMMANDATIONS	Des expertises sont identifiées et mises à jour. Elles couvrent les domaines suivants : ▸ gestion et conduite de crise ; ▸ communication de crise cyber ; ▸ gestion de projet. Des accords de non divulgation sont mis en place pour l'ensemble des experts sollicités.	Des expertises sont identifiées et mises à jour. Elles couvrent les domaines suivants : ▸ réponse à incidents[15] ; ▸ supervision de sécurité[16] ; ▸ remédiation technique ; ▸ infrastructure informatique ; ▸ annuaires et accès privilégiés (souvent Active Directory) ; ▸ restauration de données ; ▸ recouvrement de données ; ▸ solutions nuagiques ; ▸ réseaux ; ▸ administration Linux/Windows ; ▸ pare-feu. Des accords de non divulgation sont mis en place pour l'ensemble des experts sollicités.
OBJECTIF 2	**Mettre en place les capacités de réactions stratégiques face aux différentes menaces**	**Mettre en place des capacités de réactions techniques face aux différentes menaces**
RECOMMANDATIONS	Les mémos techniques sont complétés par les aspects fonctionnels et stratégiques de la gestion de crise et intègrent en particulier des listes d'actions à mener par les différentes équipes métiers. Ces mémos sont testés lors d'exercices de gestion de crise. Ils font l'objet d'une mise à jour après chaque exercice ou d'une utilisation en situation de crise.	Des outils de détection et de réponse à incident sont mis en place pour faciliter les actions de détection et d'endiguement. Des mémos techniques sur les procédures de confinement et d'éradication d'une menace cyber active sont formalisés et testés[17]. En particulier, sont pris en considération l'attaque par rançongiciel ou le déni de service. Des listes d'actions à réaliser sont formalisées pour aider les équipes techniques à mener différentes actions.

15. Le choix d'un prestataire de réponse à incident de sécurité qualifié (PRIS) est encouragé.
16. Le choix d'un prestataire de détection des incidents de sécurité qualifié est recommandé.
17. Les rapports du CERT-FR peuvent enrichir cette démarche : www.cert.ssi.gouv.fr/cti/

FICHE 6

METTRE EN PLACE DES POLICES D'ASSURANCE ADAPTÉES

La recrudescence des cyberattaques et de leurs effets sur la viabilité des organisations conduit les professionnels de l'assurance à développer une offre dédiée aux incidents cyber. Tout comme une assurance « classique », l'assurance cyber vise à compléter le niveau de protection du patrimoine d'une organisation.

Selon les conditions du contrat signé, l'assureur peut ainsi appuyer la stratégie de gestion des risques mise en place par l'organisation. Il peut aussi assister la victime d'une cyberattaque en lui faisant bénéficier d'expertises ou en lui apportant un soutien financier (remboursement du montant des pertes d'exploitation, support des coûts d'intervention d'experts, d'achat et d'installation de nouveaux SI, recours et dommages éventuellement subis par des tiers, etc.).

Il faut cependant garder à l'esprit qu'un niveau élevé de sécurité numérique doit être maintenu en parallèle et que l'ensemble des frais liés à l'incident ne pourront être couverts. Il est donc préconisé d'engager des échanges avec son assureur en amont de la crise pour vérifier les dommages couverts par le contrat en matière de reconstruction du SI (reconstruction en l'état ou reconstruction avec un renforcement), lister ses besoins et comparer les offres proposées pour adapter au mieux le niveau de couverture.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Adapter l'assurance aux besoins de l'organisation**	
RECOMMANDATIONS	Un état des lieux est mené pour identifier la couverture et les polices existantes au sein de l'organisation. Un seuil d'activation des polices d'assurance est défini. Sa mise en œuvre est testée dans le cadre d'un exercice de gestion de crise cyber. L'utilisation du contrat d'assurance fait l'objet d'un retour d'expérience après chaque activation.	Une cartographie des risques cyber est utilisée pour faciliter l'identification de l'exposition et les besoins de couverture. Les besoins en cas de crise cyber sont identifiés pour compléter les dispositifs opérationnels existants (expertise, couverture des frais, etc.). Une fiche de bonnes pratiques est formalisée pour faciliter l'utilisation de la police d'assurance en cas de crise : contacts de l'assureur, conservation des justificatifs etc.

FICHE 7
S'ENTRAÎNER POUR PRATIQUER ET S'AMÉLIORER

L'organisation d'exercices de gestion de crise cyber est un moyen efficace de sensibiliser les équipes aux enjeux cyber et d'apprendre à y faire face. En s'entraînant à affronter un enchaînement d'incidents dans des conditions réalistes, les équipes de gestion de crise impliquées développent en effet des réflexes, des méthodes et une confiance pour y faire face. Elles valident ou améliorent leurs dispositifs et leurs pratiques et prennent également l'habitude d'interagir ensemble, en dehors du cadre de travail quotidien.

L'exercice de gestion de crise[18] peut prendre diverses formes (simulation, exercice stratégique, exercice technique, exercice sur table). Ces dernières doivent être envisagées en prenant en compte les objectifs recherchés, les menaces couvertes, les périmètres techniques et métiers impliqués.

Une stratégie d'entraînement doit être définie sur plusieurs années pour permettre de créer de la cohérence dans les différents exercices tout en permettant de complexifier progressivement les scénarios, le nombre de cellules impliquées et le périmètre testé. La mobilisation des partenaires sur le périmètre testé doit également être envisagée.

18. L'utilisation du guide *Organiser un exercice de gestion de crise cyber* est préconisée : www.ssi.gouv.fr/administration/guide/organiser-un-exercice-de-gestion-de-crise-cyber/

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Définir un plan d'entraînement de crise cyber**	
RECOMMANDATIONS	Une stratégie d'entraînement de gestion de crise est définie et des exercices testant des scénarios cyber sont régulièrement organisés. Les exercices impliquent des périmètres d'impacts et des menaces différents. Le plan d'action, issu du retour d'expérience de l'exercice, fait l'objet d'un suivi pour améliorer le dispositif de crise cyber et la résilience de l'organisation.	Un volet d'entraînement opérationnel cyber et IT est intégré dans la stratégie d'entraînement. Certains exercices testent l'articulation entre les volets opérationnel et stratégique. La complexité technique des exercices est adaptée à la maturité de l'organisation. Ils tendent progressivement vers plus de réalisme pour entraîner les équipes d'investigation (type entraînement sur Cyber Range).

« Les équipes doivent être sensibilisées au dispositif de crise, via des exercices variés et à tous les niveaux, car des fiches réflexes ne servent à rien si personne ne les comprend. »

CMA CGM

PARTIE 2

RÉAGIR EFFICACEMENT EN ADOPTANT DE BONNES PRATIQUES

En temps de crise, les équipes agissent avec pour objectifs de limiter les impacts de la cyberattaque, de rétablir les services critiques dans un délai acceptable et de maintenir la confiance des parties prenantes dans l'organisation. Elles font alors face à de multiples contraintes (désorganisation de l'activité, pression médiatique et politique, remédiation technique longue et complexe, etc.), mais peuvent s'appuyer sur les dispositifs, les procédures et les outils construits et éprouvés en amont[19] de la crise pour faciliter le pilotage de l'incident et traiter ses impacts.

19. Les fiches de la première partie du guide apportent les éclairages nécessaires sur les outils à mettre en place.

Les actions des équipes s'articulent autour de quatre grandes phases de crise :

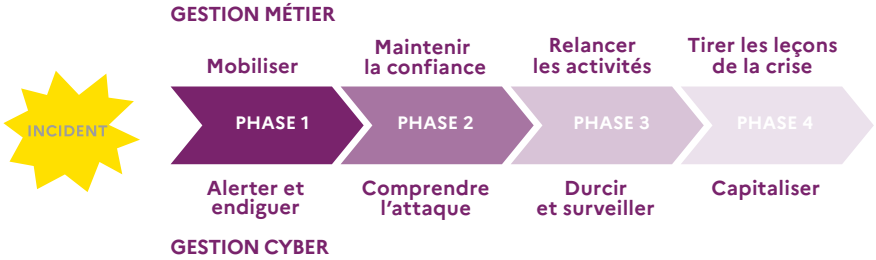
- alerter, mobiliser le personnel et arrêter la propagation de l'attaque pour protéger les bénéficiaires et l'organisation ;
- comprendre le schéma d'attaque, éjecter l'attaquant, déployer des mesures pour potentiellement travailler sans services et sans outils numériques et communiquer auprès de son écosystème pour maintenir la confiance ;
- durcir les systèmes, restaurer les applications et les données critiques et surveiller l'attaquant pour reprendre le cœur des activités ;
- revenir à la normale et faire le retour d'expérience.

Le passage d'une phase à une autre s'appuie sur des critères définis par l'organisation et s'accompagne d'un plan de communication auprès des collaborateurs, des clients, des partenaires et éventuellement des médias afin de les rassurer, de réinstaurer la confiance et d'assurer la poursuite des activités. Ces phases peuvent néanmoins se chevaucher.

Les équipes impliquées devront également s'organiser pour faire face à une épreuve d'endurance et non pas à un sprint puisque la situation de crise peut durer plusieurs semaines, avec potentiellement plusieurs mois avant une résolution complète de l'incident.

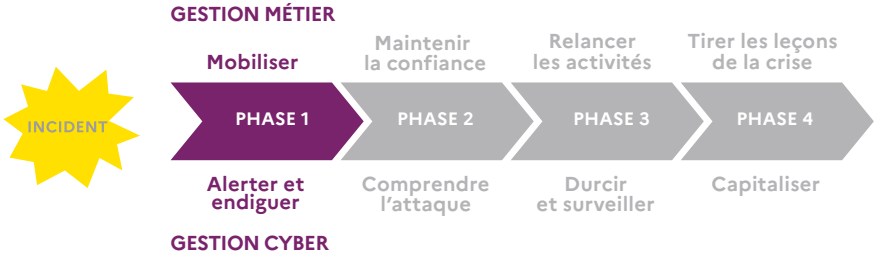
Face à ces enjeux, cette seconde partie a pour objectifs d'introduire des conseils adaptés aux différentes phases d'une crise cyber et de permettre à l'organisation de gagner en confiance dans le pilotage de cette dernière.

LES ÉTAPES D'UNE GESTION DE CRISE CYBER
(MÉTIER VERSUS CYBER)



PHASE 1

ALERTER, MOBILISER ET ENDIGUER



La détection d'un incident cyber majeur rend nécessaire de mettre en place des mesures initiales de préservation, mais implique surtout de mobiliser la structure de gestion de crise de l'organisation pouvant rassembler à la fois une cellule stratégique et plusieurs cellules opérationnelles (RH, logistique, communication etc.).

Lors de cette première phase, trois grands objectifs doivent être atteints :

- mobiliser et adapter le dispositif de crise aux enjeux et au rythme de la crise cyber (fiches 8 et 10) ;
- mettre en place les premières mesures d'**endiguement** et de continuité d'activité (fiche 9) ;
- alerter les réseaux de soutien (fiche 11).

FICHE 8
ACTIVER SON DISPOSITIF DE CRISE CYBER

Les impacts consécutifs à un ou plusieurs incidents cyber peuvent nécessiter l'activation du dispositif de crise.

Cette activation est statuée par le volet stratégique (activation par le haut) en fonction de critères préétablis. Toutefois, le dispositif opérationnel peut être mobilisé (activation par le bas) sans le volet stratégique si des actions immédiates sont nécessaires pour gérer l'incident.

À cet instant, les personnes mobilisées doivent avoir pour première intention de rassembler le personnel autour d'un objectif commun : la gestion des impacts de la crise au sein de l'organisation. Il s'agit ensuite d'identifier ensemble un plan de réaction et de défense, en fonction des impératifs techniques et métiers.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Décider de l'activation d'une cellule de crise**	**Alerter les équipes de gestion de crise de la situation**
RECOMMANDATIONS	Les fonctions décisionnelles de l'organisation prennent connaissance de l'incident via la chaîne d'alerte et analysent l'impact de la cyberattaque pour la continuité des activités de l'organisation. En fonction de critères préétablis, elles décident de déclencher « l'état de crise ». Elles définissent également des critères permettant la sortie de crise en lien avec les équipes métiers, cyber et IT.	Les équipes en charge de la gestion des incidents s'appuient sur les critères d'activation de crise cyber pour déclencher le processus d'alerte et informer les fonctions décisionnelles de l'organisation.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 2	**Mobiliser les équipes**	
RECOMMANDATIONS	À la suite du déclenchement de l'état de crise, la cellule stratégique est mise en place. Les membres identifiés se rassemblent en fonction des critères et procédures définis en amont et prennent part à leur rôle en temps de crise. Un contact permanent avec les équipes opérationnelles cyber et IT est établi. Un premier état des lieux de la situation est fait lors de la mobilisation de la cellule. Un premier « rythme de bataille » est mis en place avec des points de situation réguliers. Une main courante est ouverte pour informer les équipes des actions en cours.	Les experts nécessaires à la gestion technique de l'incident sont identifiés et rassemblés selon les besoins. Un contact permanent est établi avec les équipes décisionnelles et métiers. Un premier état des lieux de la situation est fait à la mobilisation de la cellule. Une main courante est ouverte pour informer les équipes des actions en cours.

« Dans les premières heures, il peut être difficile de distinguer un incident IT d'un incident cyber. Les équipes techniques comme métiers doivent donc être familiarisées aux enjeux cyber afin d'alerter et de mobiliser sans tarder le dispositif de crise. Il est également indispensable que les équipes de réponse à incident soient capables de détecter les signaux faibles pour couper si nécessaire les systèmes. »

CMA CGM

FICHE 9
PILOTER SON DISPOSITIF DE CRISE

Les effets d'une cyberattaque pouvant être variés et conséquents sur l'activité de l'organisation (indisponibilité des services et outils numériques, impacts de l'attaque étendus à des partenaires, etc.), il convient pour les équipes de gestion de crise cyber d'endiguer l'incident et de relancer de manière maîtrisée le fonctionnement de l'organisation. Chaque cellule va ainsi planifier un certain nombre d'actions. Mais mal coordonnées, elles peuvent être contre-productives (arrêt de systèmes essentiels, stratégie de communication inadaptée).

La cellule stratégique endosse donc le rôle de pilote de crise pour orienter le travail des équipes et atteindre les objectifs fixés.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Se focaliser sur la compréhension de l'attaque et l'étendue des impacts**	**Endiguer l'attaque**
RECOMMANDATIONS	La cellule adopte une posture de prise de décision en incertitude, en raison de l'évolution de la situation. Un équilibre est trouvé en termes de fréquence et de formalisation dans la remontée et la descente des orientations/décisions de crise, afin de laisser le temps aux équipes opérationnelles de traiter les actions demandées. Les applications, les systèmes et les périodes critiques de l'organisation sont rapidement identifiés grâce à la cartographie mise en place lors du travail préparatoire.	Les équipes cyber et IT mobilisées cherchent à circonscrire les effets de l'attaque par des mesures conservatoires. Les mesures à mettre en place pour endiguer l'attaque sont validées par la cellule stratégique si celles-ci ont des conséquences sur la continuité de l'activité (isolement, déconnexion d'applicatifs ou serveur, blocage des accès Internet, etc.). Le niveau de confiance dans l'utilisation des données et des SI est partagé avec la cellule stratégique. **Des mesures de contournement** sont prises si nécessaire.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
RECOMMANDATIONS	Une évaluation de la criticité des données compromises et du niveau de confiance dans leur utilisation ou celles des systèmes est réalisée. Les enjeux des différentes parties prenantes sont identifiés, formalisés et partagés aux cellules opérationnelles. Le dispositif de communication de crise cyber est activé (veille médiatique et sur les réseaux sociaux) et des messages de communication sont formalisés en anticipation (interne et externe) en s'appuyant sur la préparation réalisée en amont. Le paiement de la rançon doit être évité, car il entretient le système frauduleux et ne garantit pas la récupération des données.	

« Il est important que les équipes techniques ou métiers soient familiarisées aux notions d'impact cyber. La sensibilité de notre équipe dirigeante à la cybersécurité a ainsi facilité la bonne compréhension des enjeux et la prise de décision dans un moment d'incertitude. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

FICHE 10
SOUTENIR SES ÉQUIPES DE GESTION DE CRISE

La gestion des impacts d'une crise cyber pouvant s'étaler sur plusieurs semaines, il est important de mettre en place dès le début une solide organisation de crise. En fonction de l'ampleur de la crise, les équipes peuvent être sur-sollicitées par de nombreuses parties prenantes, il est donc nécessaire de les préserver et de les décharger pour qu'elles se focalisent sur des actions prioritaires. De nombreux éléments doivent ainsi être pris en compte afin de faciliter leur travail (organisation et management des équipes, format de travail – heures non ouvrées, heures ouvrées – rotations, services de restauration ou d'hôtellerie, rémunération, salles de réunions, etc.).

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Assurer un support aux volets communication et juridique**	**Créer des « équipes » cyber**
RECOMMANDATIONS	Une cartographie des actions menées, en particulier celles en lien avec les clients, partenaires et fournisseurs, est réalisée. Dans la stratégie de communication, les principaux éléments de langage sont adaptés en s'appuyant sur les éléments formalisés en phase de préparation. Des communications sont réalisées pour informer en interne sur la progression des actions, si nécessaire. Un outil de questions/réponses est mis en place. L'équipe juridique est mobilisée et les obligations auprès des partenaires, clients, fournisseurs qui ne peuvent pas être respectées sont identifiées.	Les collaborateurs sans activité peuvent être mobilisés pour fournir de l'aide sur les différentes actions à réaliser. Le travail peut être organisé sous forme d'équipes-projet, afin de répondre à plusieurs objectifs dans un délai réduit.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
	Si nécessaire, une communication vers les partenaires est effectuée en utilisant les canaux prédéfinis et dans les délais définis dans les contrats.	
OBJECTIF 2	**Mettre en place un support RH adapté**	
RECOMMANDATIONS	Le roulement des équipes est anticipé et le nombre d'heures des collaborateurs est suivi afin de préserver leur capacité à opérer dans la durée et de régulariser leur temps de travail. Les prestataires mobilisés font également un suivi équivalent pour les ressources utilisées. Une personne est dédiée à ce suivi.	
OBJECTIF 3	**Organiser les aspects logistiques de la gestion de crise**	
RECOMMANDATIONS	De la restauration, des logements et des moyens de transports sont mis à disposition des équipes impliquées (notamment en dehors des jours/heures ouvrés habituels). Un réaménagement temporaire d'une partie des locaux est effectué si nécessaire. Les besoins familiaux des personnes mobilisées sont pris en compte et des solutions peuvent être mises en place (garde d'enfants, horaires adaptés, etc.) L'accès aux bâtiments 24/7 (badges, etc.) est mis en place. Si des prestataires sont mobilisés, une liste nominative des personnes est communiquée aux équipes logistiques pour fournir des badges et un accès aux locaux. Des salles de réunions permettant aux différentes cellules de se retrouver et de travailler ensemble sont mises à disposition. Des outils numériques adaptés au contexte sont fournis. Une personne est dédiée au suivi de la logistique.	

« Il a fallu soutenir 24/7 les équipes intervenants dans la gestion de crise, que ce soit tant au niveau professionnel, en les protégeant des sur-sollicitations internes et externes, qu'au niveau personnel afin de faciliter l'organisation individuelle. Le soutien humain des soignants et des directeurs les a également aidés à rester motivés et à tenir le rythme. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

FICHE 11
ACTIVER SES RÉSEAUX DE SOUTIEN

La gestion des impacts d'une crise cyber implique de faire appel à un réseau d'experts (assureurs, CERT, équipes de forensics, etc.) qui appuieront les équipes dans la réalisation de leurs actions. Pour faciliter leur mobilisation, il convient notamment de s'appuyer sur les annuaires mis en place en amont. En fonction des obligations réglementaires auxquelles l'organisation est soumise, il est également important de notifier les autorités compétentes : elles peuvent dans certains cas proposer un soutien à l'organisation victime d'une cyberattaque.

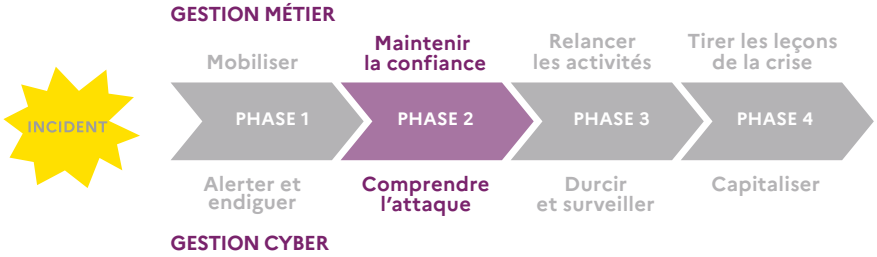
	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Activer son assurance cyber**	
RECOMMANDATIONS	L'assurance cyber est activée sur décision de la cellule stratégique, selon les critères préétablis. Les expertises à mobiliser via l'assurance sont identifiées et notifiées à l'assureur. La main courante est utilisée pour le suivi et la centralisation des actions et des frais liés à la gestion de la crise.	Les équipes identifient le support technique nécessaire, en particulier sur les volets d'investigation et reconstruction. Une synthèse des évènements et de la situation actuelle est formalisée pour le partager avec l'assureur.
OBJECTIF 2	**Mobiliser et centraliser les demandes de renfort**	
RECOMMANDATIONS	Les équipes métiers et cyber centralisent leurs besoins en ressources. Des personnes en charge de coordonner le réseau des experts sont mobilisées et mènent cette action. Elles contactent les experts qui ont été identifiés en amont ou se chargent de les identifier. En concertation avec le volet logistique, elles prennent en charge l'accueil des experts.	Le processus d'identification des besoins est conduit à intervalles réguliers, en particulier pendant les phases d'investigation et de reconstruction. Une cellule (ou personne) centralisant les demandes de ressources est mise en place. Elle gère la logistique et répond aux demandes. En cas de présence d'un CERT/CSIRT, une information peut être partagée à d'autres CERT/CSIRT (e.g réseau sectoriel, cercle de confiance, etc.).

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 3	**Déclarer son incident auprès des autorités compétentes** En fonction du statut de l'organisation, plusieurs actions peuvent être entreprises[20] et donner lieu à des préconisations de la part des autorités.	
RECOMMANDATIONS	En lien avec les équipes juridiques, un dépôt de plainte est envisagé. Les actions de déclaration d'incident (ANSSI, CNIL, autorités judiciaires) sont centralisées et coordonnées par la cellule stratégique. En cas de violation des données personnelles (règlement général sur la protection des données), une notification de l'incident est réalisée par le délégué à la protection des données. Dans le cadre d'une crise d'ampleur internationale, les équipes juridiques prennent en compte la législation en vigueur et coordonnent la notification d'incident aux autorités locales.	Les équipes cyber et IT partagent les informations nécessaires à la déclaration d'incident. Les preuves de compromission (serveurs, données) sont conservées pour la justice (si judiciarisation) et pour l'assureur (si activation d'un contrat d'assurance). En cas de judiciarisation, un huissier spécialisé est sollicité pour établir le constat. En fonction des obligations légales, une déclaration d'incident est réalisée et les éléments de compromission sont partagés avec l'ANSSI.

20. www.ssi.gouv.fr/en-cas-dincident/

PHASE 2

MAINTENIR LA CONFIANCE ET COMPRENDRE L'ATTAQUE



Une fois le dispositif de crise activé et les équipes mobilisées, il s'agit de limiter au maximum les impacts immédiats du dysfonctionnement des SI sur l'activité de l'organisation. Pour y parvenir, les équipes de gestion de crise aspirent donc à :

- communiquer sur la situation pour rassurer les partenaires de confiance (fiche 12) ;
- comprendre le déroulé de l'attaque pour définir le périmètre de compromission cyber et métier (fiche 13).

FICHE 12
COMMUNIQUER EFFICACEMENT

En fonction de son type et de son ampleur, les impacts d'une cyberattaque peuvent être immédiatement visibles, obligeant l'organisation à communiquer rapidement sur la situation en interne et en externe. Le nombre d'acteurs impliqués directement ou indirectement dans une crise cyber rend parfois difficile la cohérence des canaux de communication pour maîtriser le discours global, tant le sujet cyber est technique et évolutif.

Il convient alors de construire une stratégie de communication et des éléments de langage associés avec l'aide des équipes communication, cyber et IT, pour informer, rassurer, mobiliser et protéger l'image de l'organisation.

Cette stratégie s'appuie sur une analyse de la situation et les éléments d'ores et déjà préparés[21], mais également sur une analyse de risque médiatique intégrant les éléments relatifs à la situation opérationnelle (issus des équipes cyber et IT) et des enjeux de réputation et de confiance définis avec la cellule stratégique. Elle doit ainsi intégrer les impacts de l'incident, le contexte socio-politique (risques, sujets d'actualité) et les points de vigilance liés à l'organisation (notoriété, actualité du secteur, rachat, communication financière etc.).

21. Se référer à la première partie du guide, en particulier la fiche 3 : formaliser une stratégie de communication de crise cyber.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Adapter son plan de communication à la situation**	**Informer la cellule stratégique de la situation**
RECOMMANDATIONS	Deux plans sont construits : un plan de communication interne et un plan de communication externe. Un rythme de communication adapté aux objectifs stratégiques est mis en place. Des relais de communication (presse, web, communication interne) sont mobilisés. Des relais régionaux/internationaux sont identifiés et mobilisés en fonction de la taille et de l'activité de l'organisation. Un ou des porte-paroles (formés aux enjeux cyber) sont mobilisés pour permettre aux experts de se focaliser sur la gestion de la crise. En cas d'indisponibilité des canaux de communication, les communications sont diffusées sur les réseaux alternatifs mis en place (communication physique, site temporaire, boîte vocale temporaire, etc.).	Les actions effectuées et celles en cours sont communiquées régulièrement à la cellule stratégique. Les incertitudes et les zones d'ombres sont en particulier partagées. Les équipes cyber et IT aident les équipes communication à vulgariser certains éléments techniques afin de s'adapter à des publics non-experts.

OBJECTIF 2	Rassurer ses parties prenantes et les médias	Rassurer les équipes techniques des parties prenantes
RECOMMANDATIONS	Des communications régulières sont effectuées pour tenir informé les parties prenantes de l'évolution de la situation, maîtriser les informations partagées et éviter la propagation de rumeurs. Les éléments de langage sont formalisés et validés par les équipes communication et juridique. Un point de contact unique centralise les sollicitations de presse. Une cellule de veille médiatique est mise en place pour faciliter le suivi des impacts de la communication et anticiper les actions. Une communication descendante est mise en place pour fournir de la visibilité sur l'évolution de la situation et les jalons majeurs pour favoriser l'adhésion. Un outil de questions/réponses est mis en place.	Les sollicitations des clients, des partenaires et des autorités pour disposer d'éléments techniques complémentaires sur l'attaque font l'objet d'un suivi centralisé. Un canal sortant unique est mis en place pour répondre à ces sollicitations.

« La direction de la communication nous a accompagnés pour définir une stratégie de communication dès les premières heures de la crise. Nous avons travaillé les messages en fonction des publics et avons pu utiliser les outils qui restaient à notre disposition. Les relais de l'information dans l'entreprise (DG, commerciaux, RH, financiers, juristes,etc.) ont reçu les informations nécessaires pour pouvoir répondre aux questions des collaborateurs, des clients et des partenaires (fournisseurs, assurances, banques, etc.) et nous avons aussi mis en place des ''hotlines'' dédiées. »

Bouygues Construction

« En cas d'attaque, il faut s'attendre à recevoir de nombreuses sollicitations de la presse. L'implication des équipes de communication aux côtés des équipes opérationnelles permet de centraliser les demandes presse, construire des éléments de langage ou répondre aux questions afin de les décharger d'un poids conséquent. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

FICHE 13
CONDUIRE L'INVESTIGATION NUMÉRIQUE

Comprendre les actions de l'attaquant et ce qui a pu le motiver à viser l'organisation (données sensibles, appât du gain, etc.) est une étape essentielle pour la résolution de la crise puisqu'elle permet de prioriser les actions de remédiation et d'engager une stratégie de reconstruction pour recréer un cœur de confiance. Elle atteste également des failles exploitées pour s'introduire dans les systèmes de l'organisation et oblige *in fine* les équipes à rehausser le niveau de cybersécurité.

Elle permet enfin de comprendre l'étendue de la compromission et de la durée potentielle de l'indisponibilité des services et des outils, de manière à ce que les équipes métiers mettent en place la meilleure stratégie de continuité d'activité.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Appuyer la stratégie d'investigation**	**Établir la stratégie d'investigation**
RECOMMANDATIONS	Un équilibre est trouvé entre la rapidité de la remise en production des **applicatifs métiers** et le maintien d'un niveau de sécurisation adapté. Un arbitrage sur la remise en fonction prioritaire des applicatifs métiers est réalisé. Il s'appuie sur le niveau de dangerosité qu'induit la relance des serveurs/postes, du niveau de sécurisation du **cœur de confiance** et de la capacité à maintenir ce dernier dans le temps. Le niveau de complexité des investigations et leur longueur sont pris en considération dans les arbitrages. Le rythme du plan de reconstruction des serveurs et des postes est défini en s'assurant de l'absence de traces de l'attaque sur les serveurs et les postes. En s'appuyant sur la cartographie des actifs sensibles, des orientations sont données sur les systèmes et applications sur lesquels investiguer en priorité.	Les investigations se concentrent dans un premier temps sur l'identification du périmètre de compromission, les vecteurs potentiels d'infection et les fonctions malveillantes. Des résultats intermédiaires sont partagés. Ils sont vulgarisés et contextualisés et doivent être clairs pour éviter les mauvaises interprétations. Dès le début, une communication est réalisée au sein de l'entité sur le fait que le « patient 0 » ne sera peut-être jamais identifié et que certaines questions resteront sans réponses. La seule priorité doit être de relancer les services dans des conditions de sécurité acceptables. Les actions de l'attaquant font l'objet d'un document synthétique et facilement adressable au niveau stratégique. Les analyses peuvent être dévolues à un prestataire (PRIS) qui se concentre sur toutes les actions réalisées par l'attaquant. Des arbitrages sont demandés sur les orientations des investigations, en fonction de la sensibilité des actifs.

OBJECTIF 2	Focaliser son attention sur l'attaque plutôt que sur un/des responsable(s)	Organiser les investigations
RECOMMANDATIONS	L'action d'investigation menée par les équipes cyber est soutenue dans le but de comprendre l'étendue de la compromission et de prioriser les actions de remédiation. La recherche d'un coupable n'est pas une priorité pour la cellule stratégique, qui focalise ses efforts sur le maintien de l'activité.	Les investigations ne sont pas focalisées sur l'ensemble des vulnérabilités mais sur le **chemin de compromission** ayant permis la réalisation de l'attaque. L'identification du périmètre de compromission pour alimenter le **plan de défense** est une priorité. Une organisation dédiée est mise en place pour piloter l'ensemble des collectes des journaux et la réalisation des actions connexes aux investigations. Les différentes collectes sont centralisées pour les distribuer aux parties prenantes : équipes cyber et IT, prestataires, autorités, etc. Le délai de rétention des journaux des SI est ajusté, les investigations pouvant potentiellement durer pendant plusieurs semaines. Tous les prestataires mobilisés travaillent ensemble de façon coordonnée avec des objectifs et des périmètres clairement définis.

« Dès le début de la crise, notre priorité était très claire : poursuivre l'activité sur les chantiers. Pour cela, nous avons rétabli en premier le paiement de nos collaborateurs et de nos fournisseurs. Nous avons dû faire preuve d'agilité en mobilisant des collaborateurs de province pour les faire travailler sur un réseau fermé. Nous nous sommes également appuyés sur les initiatives de collaborateurs pour mettre en place des mesures alternatives. Pour rétablir au plus vite l'activité, nous avons dû faire preuve de souplesse, toutefois jamais sans garde-fou pour éviter une nouvelle compromission. »

Bouygues Construction

FICHE 14
METTRE EN PLACE UN MODE DE FONCTIONNEMENT DÉGRADÉ POUR LES MÉTIERS IMPACTÉS

Lors d'une crise cyber, un rançongiciel peut rendre indisponible l'ensemble des services et outils numériques de l'organisation, obligeant ainsi les métiers à adapter leurs activités. Dans d'autres cas, les mesures d'endiguement ou de remédiation des équipes IT et cyber peuvent rendre partiellement indisponibles certains outils du fait d'actions d'isolation ou de déconnexion.

La stratégie de gestion de crise cyber, adossée aux dispositifs de continuité d'activité doit ainsi prévoir des solutions opérationnelles permettant de maintenir sur une durée parfois très longue le fonctionnement de l'organisation sans outils numériques.

22. Se référer à la première partie du guide pour la définition des dispositifs adaptés à la menace cyber.
23. Se référer au site du collectif NoMoreRansom qui propose plusieurs outils de déchiffrement de fichiers : www.nomoreransom.org/fr/

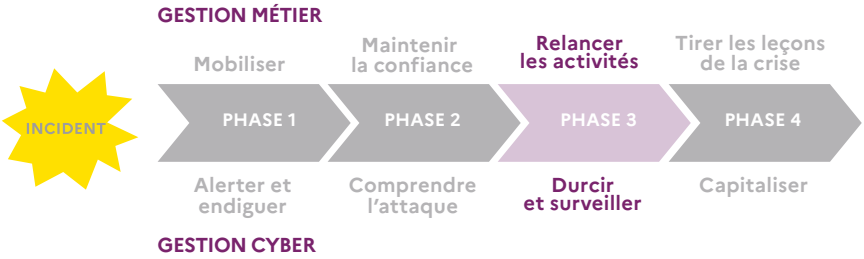
	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Définir les modes d'utilisation des solutions de contournement**	**Soutenir le déploiement de solutions de contournement**
RECOMMANDATIONS	Les solutions de contournement et les capacités opérationnelles de résilience identifiées au préalable pour maintenir une activité dégradée sont mises en œuvre (solution nuagique, prestataire, papier, moyens personnels, etc.). Une communication interne sur les solutions choisies est réalisée pour garantir leur bonne compréhension et leur bonne utilisation. Si nécessaire, une communication est réalisée auprès des clients sur les règles d'utilisation des services et des outils temporaires.	La possibilité d'utiliser des sauvegardes saines pour rétablir au plus vite la situation est étudiée. L'utilisation d'outils de déchiffrement libres d'accès (sans rançon à payer) est également envisagée. Les équipes cyber et IT recommandent des mesures de contournement numériques à envisager et facilitent leur mise en place de façon sécurisée. Pour mener ces actions, une coordination renforcée est mise en place au niveau des équipes locales, en particulier IT. Les dates envisagées de remise en service des applications sont partagées pour permettre aux équipes métiers de se projeter en particulier sur la durée de maintien des modes dégradés.

« Le partage progressif des résultats des investigations a été indispensable pour que les managers se représentent les effets de la crise sur l'activité métier. Les experts apportent des réponses aux nombreuses questions et il ne faut pas hésiter à passer par des références imagées pour aider à la compréhension de la situation. »

CMA CGM

PHASE 3

RELANCER LES ACTIVITÉS MÉTIERS ET DURCIR LES SYSTÈMES D'INFORMATION



Les périmètres de compromission identifiés et les parties prenantes informées, les équipes de gestion de crise doivent agir pour revenir à une situation normale. Pour y parvenir, elles doivent réussir à :

- mettre en œuvre des actions de sécurisation et de durcissement pour permettre la reprise d'activité (fiche 15) ;
- adapter l'activité de l'organisation aux contraintes persistantes (fiche 16).

FICHE 15
DURCIR ET REMÉDIER

Une fois le chemin et le périmètre de compromission de l'attaque identifiés, il s'agit de protéger les SI de l'organisation contre de nouvelles attaques. Ces nouvelles mesures peuvent entraîner une modification importante des pratiques, notamment d'administration, et des modes de fonctionnement des métiers dans l'utilisation des services et des outils numériques. Dès lors, un effort de pédagogie est nécessaire pour expliquer, à tous les niveaux, les changements parfois profonds qui seront effectués pour éviter une nouvelle compromission des systèmes et parvenir à une sortie de crise.

Les équipes métiers, cyber et IT doivent ainsi travailler de concert pour adapter le rythme de leurs actions et surmonter cette étape clé de la gestion d'une crise cyber.

« Malgré l'urgence de remédier, une certaine patience a été de mise. La remédiation de l'incident affectant l'environnement numérique doit se faire à travers une analyse concrète des impacts, des motifs et des causes sous-jacentes. Des corrections de court terme sont alors menées, mais également des transformations plus complexes. Des parties tierces peuvent ainsi être mobilisées le week-end et la nuit et il faut s'assurer que leurs processus soient adaptés à ce nouveau rythme de crise. »

CMA CGM

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Objectiver les orientations sur le durcissement et la remédiation**	**Reprendre le contrôle des systèmes et durcir pour empêcher de nouvelles compromissions**
RECOMMANDATIONS	Les actions de durcissement et de remédiation sont planifiées pour organiser au mieux le travail des équipes opérationnelles. Ces actions valident des objectifs définis. Les risques à ne pas réaliser certaines actions de durcissement et de remédiation sont évalués et pris en compte. Les objectifs du plan d'action et du planning associé (en particulier les remises en route d'application métier) sont ajustés en fonction des contraintes techniques de la remédiation. Un changement de **pratiques d'administration** et de gestion des SI peut être nécessaire pour renforcer la sécurité. Il est alors promu par les équipes décisionnelles. Le PRA est adapté en fonction des avancées des actions d'investigation et de remédiation en cours et à venir. L'ensemble des décisions prises font l'objet d'un suivi et permettent de valider les critères de sortie de crise.	Un plan de durcissement et de remédiation est élaboré de façon itérative en fonction des retours des investigations numériques. Il permet en particulier de neutraliser les vecteurs d'infection et de propagation. Des mesures de durcissement globales sont mises en place pour isoler l'attaquant si celui-ci parvient à maintenir son accès à certaines parties du SI. En cas de mesures structurantes, les impacts sur les SI et les métiers sont identifiés et validés en amont de leur déploiement.

OBJECTIF 2	Reconstruire un cœur de confiance
RECOMMANDATIONS	Une bulle sécurisée est mise en place et les services à réintégrer sont priorisés par la cellule stratégique. Une surveillance des systèmes est mise en place, en particulier ceux identifiés comme précédemment compromis par l'investigation. Un accompagnement sur les nouvelles pratiques de sécurité dans les équipes de production informatique est effectué, soutenu par la cellule stratégique. Une coordination renforcée est mise en place au niveau des équipes locales, en particulier IT. Un processus de validation permettant d'assurer la bonne application des mesures de sécurité avant la remise en production d'un système ou d'une application est également formalisé.

FICHE 16
PRÉPARER ET INDUSTRIALISER LA RECONSTRUCTION

Les SI étant compromis, une reconstruction de ces derniers doit être envisagée avant de revenir à la normale. L'objectif est de remettre en production des outils et des systèmes mieux sécurisés, en respectant un standard de sécurité plus élevé afin de limiter le risque d'une nouvelle compromission.

Cette phase de la gestion de crise cyber est particulièrement consommatrice en ressources humaines comme financières. La priorité doit donc être donnée aux systèmes les plus critiques pour le fonctionnement des métiers ou pour respecter des périodes critiques de l'organisation (paiement des salaires, livraisons, etc.).

L'application de nouvelles mesures de sécurité pouvant entraîner des ralentissements dans la reconstruction, c'est au volet stratégique de rester cohérent et d'éviter de favoriser l'application de mesures plus pratiques, mais moins sécurisées. Une attention particulière est ainsi apportée à la bonne application des règles et toute dérogation doit faire l'objet d'une prise de connaissance par la cellule stratégique avec une acceptation formelle des risques potentiels associés.

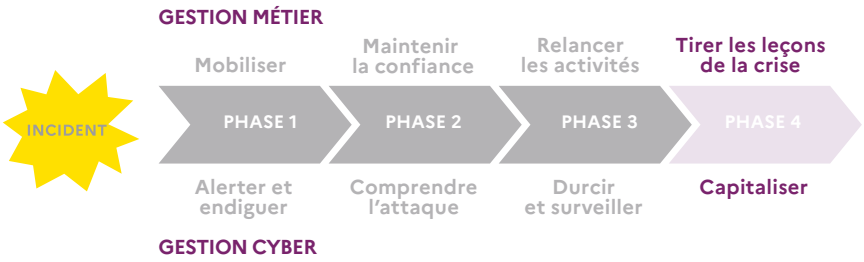
	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Organiser et adapter le comportement des utilisateurs**	**Sécuriser l'industrialisation de la reconstruction**
RECOMMANDATIONS	Une priorisation (P0 – P1 – P2 – P3) des applications et des systèmes à reconstruire est réalisée (en fonction de la criticité) et validée. Le support en ressources est renforcé pour assurer la reconstruction IT, le cas échéant en travail posté (24 h/24). De la visibilité et de la transparence sur le réalisme de la réouverture des applications métiers sont demandées par les équipes décisionnelles aux équipes techniques cyber et IT. Les métiers sont mobilisés pour réaliser des tests utilisateurs avant la remise en production des applications. Des communications aux utilisateurs et aux parties prenantes externes sont réalisées quand les services rouvrent. Une attention particulière est portée à ce que les mesures prises ne laissent pas penser à une sortie de crise tant que les critères ne sont pas atteints.	Une stratégie de reconstruction est définie : elle s'appuie sur des sauvegardes saines. Cette stratégie comprend un volet sur la restauration des données. Le risque d'une restauration partielle des données, lié à des sauvegardes désynchronisées est pris en compte. Un suivi des différentes étapes du processus est effectué. Celui-ci est régulièrement partagé à la cellule opérationnelle cyber et IT et la cellule stratégique. Des dates prévisionnelles de remise en service des applications sont également indiquées pour conserver la mobilisation des équipes. Une coordination renforcée est mise en œuvre entre les équipes en charge du durcissement et de la remédiation et celles en charge de la reconstruction afin de faire appliquer les mesures de cybersécurité. En cas de reconstruction en travail posté, les équipes du volet remédiation assurent un équivalent pour répondre aux demandes de validation.

« De nombreux postes de travail devaient être réinstallés, il a donc fallu prioriser la relance des activités les plus critiques. Il a été décidé que la crise serait clôturée uniquement quand l'ensemble des établissements de santé seraient opérationnels. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

PHASE 4

TIRER LES LEÇONS DE LA CRISE ET CAPITALISER



Les actions de remédiation et de reprise d'activité laissant entrevoir un retour à plus de stabilité, les équipes de gestion de crise doivent enfin envisager une sortie de crise. Pour atteindre ce dernier objectif, il est important qu'elles réussissent à :

- définir et organiser leur plan de sortie de crise (fiche 17) ;
- tirer parti de l'expérience de crise pour progresser (fiche 18).

FICHE 17
ORGANISER SA SORTIE DE CRISE

La fin d'une période de crise cyber ne signifie pas que l'organisation va retrouver un fonctionnement opérationnel dès cet instant, puisque la reconstruction et le durcissement de l'ensemble des systèmes peuvent prendre plusieurs mois. La sortie de crise s'envisage au contraire lorsque les activités essentielles de l'organisation peuvent reprendre de manière habituelle. Pour cela, plusieurs conditions doivent être réunies et il revient à la cellule stratégique de les définir.

« Nous avons rapidement formalisé des critères de sortie de crise pour passer en gestion courante. Trois principaux critères ont été établis : les applications prioritaires sont fonctionnelles, les sauvegardes sont en état de fonctionnement, la reconnexion des sites internationaux est effective. »

Bouygues Construction

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Adapter des seuils de sortie de crise**	**Permettre la reprise progressive des outils numériques**
RECOMMANDATIONS	Les conditions nécessaires à la sortie de crise, prédéfinies au début de l'incident, sont réévaluées. Elles prennent en compte, en particulier, les connaissances sur l'attaque, le rétablissement des services et la remise en production des systèmes affectés. Un plan d'action permettant de capitaliser sur l'ensemble des chantiers qui seront à mener après la crise est formalisé. Une communication est envoyée à l'ensemble des équipes pour informer de la sortie de crise. Les obligations réglementaires de déclaration post-crise sont identifiées et réalisées. Un point sur les ressources humaines est effectué en particulier pour les régularisations potentielles (indemnisations, repos). Les équipes sont remerciées pour leur travail et leur mobilisation.	Les solutions de contournement sont évaluées pour être maintenues ou supprimées en concertation avec les équipes métiers. Le **registre des risques/des dérogations** est fiabilisé pour alimenter la sortie de crise. Le rythme de mobilisation des équipes est revu progressivement à la baisse. Une surveillance des SI est maintenue, en particulier sur le chemin d'attaque. Les équipes sont remerciées pour leur travail et leur mobilisation.

FICHE 18
TIRER LES LEÇONS DE LA CRISE

À la suite d'une crise, les équipes sont tentées de reprendre rapidement une activité normale. Pour autant, cette période de transition est le meilleur moment pour revenir sur la conduite de la crise et capitaliser sur ce qui a été vécu et ce qui pourrait être amélioré. Le retour d'expérience (RETEX) participe notamment à renforcer la résilience de l'organisation, en mettant en avant les points forts et les axes d'amélioration suite aux dysfonctionnements constatés. Il permet en particulier de pérenniser certains dispositifs de gestion de crise qui ont été jugés efficaces.

Les thèmes qui peuvent être abordés dans le cadre du RETEX concernent :

- la gouvernance et le processus de gestion de crise ;
- la communication de crise ;
- le processus de prise de décision et de suivi des actions ;
- les capacités techniques et opérationnelles ;
- les interactions entre les équipes mobilisées dans la crise ;
- les interactions avec les parties prenantes extérieures.

Le RETEX doit s'organiser après la clôture de la crise 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 ; un retour d'expérience « à froid » permettant de présenter une synthèse des observations, des recommandations et le plan d'action associé.

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
OBJECTIF 1	**Organiser le RETEX**	
RECOMMANDATIONS	La cellule stratégique identifie une équipe en charge de mener un RETEX de la gestion de la crise. L'équipe en charge du RETEX identifie les acteurs à interroger et la grille d'entretien, organise les aspects pratiques de la conduite de l'exercice (calendrier, méthode, document de synthèse, animation). Le RETEX est organisé pour le volet stratégique et opérationnel. Un délai maximum de 30 jours est prévu entre la fin de la crise et la fin du processus RETEX. Un rapport d'investigation numérique et sa synthèse (à destination des équipes dirigeantes) sont demandés aux prestataires mobilisés.	
OBJECTIF 2	**Valoriser le RETEX**	
RECOMMANDATIONS	L'équipe en charge du RETEX utilise les données récoltées pour construire un rapport identifiant les actions à mener pour améliorer le dispositif de gestion de crise. La restitution est organisée à plusieurs niveaux, par exemple en diffusant une synthèse à la direction générale et un document plus complet aux équipes de gestion de crise. Les axes d'amélioration font l'objet d'un suivi spécifique, via un plan d'action.	

« Les retours d'expériences ont été menés avec toutes les équipes pour questionner et améliorer les pratiques et les procédures de nos métiers en temps froid et en temps chaud. Aujourd'hui, l'enjeu est d'être encore plus résilient en cas de crise longue. »

L'Hôpital Nord-Ouest - Villefranche-sur-Saône

ANNEXE 1

BOÎTE À OUTILS DE GESTION DE CRISE CYBER

Cette liste non exhaustive d'outils et de procédures pouvant être mis en place en amont de tout incident peut vous aider à parfaire votre dispositif de gestion de crise cyber. Un maintien en conditions opérationnelles de ces derniers est indispensable. Les solutions et les outils qualifiés par l'ANSSI peuvent être utilisés.

OUTILS GÉNÉRAUX	OUTILS SPÉCIFIQUES
▸ Salle de crise physique ou virtuelle ▸ Annuaire de crise (personnes internes et externes) accessible en cas de black-out ▸ Outil de suivi des actions ▸ Outil de main courante ▸ Outils de communication résilients/ hors réseau : adresses mails génériques, tchat, visioconférence, téléphone fixes ou mobiles, etc. ▸ Fiches-rôle ▸ Fiches réflexes ▸ Contrats d'assurance	▸ Critères de déclenchement d'une cellule de crise cyber ▸ PCA et PRA cyber ▸ Cartographie des systèmes et des services critiques ▸ Liste des experts et des prestataires à contacter ▸ Plan de communication de crise cyber ▸ Liste des parties prenantes à informer (clients, fournisseurs, autorités) ▸ Registre des risques et des dérogations ▸ Ordinateur hors réseau

ANNEXE 2

OBJECTIFS DE LA GESTION D'UNE CRISE CYBER

NOM DE LA FICHE
Fiche 1 : connaître et maîtriser ses systèmes d'information
Fiche 2 : mettre en place un socle de capacités opérationnelles garantissant un niveau adapté de résilience numérique
Fiche 3 : formaliser une stratégie de communication de crise cyber
Fiche 4 : adapter son organisation de crise au scénario cyber
Fiche 5 : préparer ses capacités de réponse à incident
Fiche 6 : mettre en place des polices d'assurance adaptées
Fiche 7 : s'entraîner pour pratiquer et s'améliorer
Fiche 8 : activer son dispositif de crise cyber
Fiche 9 : piloter son dispositif de crise
Fiche 10 : soutenir ses équipes de gestion de crise
Fiche 11 : activer ses réseaux de soutien

OBJECTIFS STRATÉGIQUES	OBJECTIFS OPÉRATIONNELS
Cartographier ses applications et ses ressources métiers critiques	Cartographier ses SI
Adapter le plan de continuité d'activité au scénario de crise cyber Réaliser un plan de reprise d'activité pour le scénario cyber Mettre en place des outils de conduite de crise résilients	
Établir une liste des parties prenantes à contacter Anticiper la stratégie de communication de crise	
Mettre en place des critères et des procédures d'activation des cellules de crise Organiser ses cellules de crise cyber	
Identifier les experts à solliciter en temps de crise	
Mettre en place des capacités de réactions stratégiques face aux différentes menaces	Mettre en place des capacités de réactions techniques face aux différentes menaces
Adapter l'assurance aux besoins de l'organisation	
Définir un plan d'entraînement de crise cyber	
Décider de l'activation d'une cellule de crise	Alerter les équipes de gestion de crise de la situation
Mobiliser les équipes	
Se focaliser sur la compréhension de l'attaque et l'étendue des impacts	Endiguer l'attaque
Assurer un support aux volets communication et juridique Mettre en place un support RH adapté Organiser les aspects logistiques de la gestion de crise	Créer des « équipes » cyber
Activer son assurance cyber Mobiliser et centraliser les demandes de renfort Déclarer son incident auprès des autorités compétentes	

	Adapter son plan de communication à la situation Rassurer ses parties prenantes et les médias	Informer la cellule stratégique de la situation Rassurer les équipes techniques des parties prenantes
	Appuyer la stratégie d'investigation Focaliser son attention sur l'attaque plutôt que sur un/des responsable(s)	Établir la stratégie d'investigation Organiser les investigations
	Définir les modes d'utilisation des solutions de contournement	Soutenir le déploiement de solutions de contournement
	Objectiver les orientations sur le durcissement et la remédiation	Reprendre le contrôle des systèmes et durcir pour empêcher de nouvelles compromissions Reconstruire un cœur de confiance
	Organiser et adapter le comportement des utilisateurs	Sécuriser l'industrialisation de la reconstruction
	Adapter des seuils de sortie de crise	Permettre la reprise progressive des outils numériques
	Organiser le RETEX Valoriser le RETEX	

GLOSSAIRE

ACTIVE DIRECTORY :
annuaire de service Windows offrant un système centralisé et normalisé de gestion des identités et des accès.

BILAN D'IMPACT SUR L'ACTIVITÉ :
processus identifiant les activités critiques et prioritaire d'une organisation et déterminant les ressources minimales nécessaires pour satisfaire les exigences de continuité d'activité.

***COMPUTER SECURITY INCIDENT RESPONSE TEAM* (CSIRT) OU CERT :**
centre d'alerte, de traitement et de réaction aux cyberattaques destiné aux entreprises, aux administrations ou aux autorités.

DURCISSEMENT : action de renforcement de la sécurité des SI dans le but d'éviter une nouvelle intrusion de la part de l'attaquant.

DURÉE MAXIMUM D'INTERRUPTION D'ACTIVITÉ (*RECOVERY TIME OBJECTIVE*) : métrique déterminant le délai maximal tolérable nécessaire pour remettre en ligne les systèmes critiques.

ENDIGUEMENT : action de protection visant à stopper la propagation d'un attaquant sur des SI.

FAILLE EXPLOITÉE : faiblesse dans un système informationnel permettant à un attaquant de porter atteinte à l'intégrité de ce système.

INFRASTRUCTURE DE GESTION DES CLÉS : ensemble de moyens techniques et organisationnels permettant d'établir une forte garantie de confiance dans la validité d'une identité numérique.

ISOLEMENT : procédure de cloisonnement ou de déconnexion de systèmes informationnels du réseau Internet ou du réseau Intranet à la suite d'une cyberattaque pour en éviter sa propagation.

MESURE DE CONTOURNEMENT :
non-application d'une règle nominale de fonctionnement d'un système informationnel ou technologie impliquant son fonctionnement en mode dégradé.

PLAN DE CONTINUITÉ D'ACTIVITÉ, PCA (ISO 22301) : ensemble de procédures documentées servant de guides aux entités pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation.

PLAN DE DÉFENSE : stratégie mise en place dans le but de protéger les systèmes informationnels d'une cyberattaque.

PLAN DE REPRISE D'ACTIVITÉ, PRA (ISO 22301) : procédures documentées permettant aux entités de rétablir et de reprendre leurs activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident.

PRATIQUES D'ADMINISTRATION : processus d'installation et paramétrage, de mises à jour, de supervision, de contraintes d'accès, permettant de sécuriser les systèmes informationnels.

REMÉDIATION : processus de limitation des effets de l'incident sur les SI.

SAUVEGARDE SAINE : processus d'enregistrement de données sur des serveurs déconnectés conduit et testé régulièrement permettant d'assurer l'intégrité et la disponibilité des données.

SCÉNARIO CYBER DE RÉFÉRENCE : scénario de risque pour l'organisation, évalué en fonction de la gravité et la vraisemblance de l'impact du risque.

SERVICES NUMÉRIQUES : services mis en place par une organisation auxquels sont associés ses systèmes d'information et ceux de ses prestataires ou partenaires.

SYSTÈME D'INFORMATION : ensemble des ressources (matérielles ou logicielles) et dispositifs d'une organisation permettant de collecter, de stocker et d'échanger les informations nécessaires à son fonctionnement.

SYSTÈME DE NOM DE DOMAINE (*DOMAIN NAME SYSTEM*, DNS) : service permettant d'établir une correspondance entre un nom de domaine et une adresse IP.

TEMPS D'ARRÊT MAXIMAL TOLÉRABLE (*MAXIMUM TOLERABLE DOWNTIME*) : métrique déterminant la durée totale pendant laquelle un processus d'entreprise peut être perturbé sans entraîner de conséquences inacceptables.

TEMPS DE RÉCUPÉRATION DES DONNÉES (*WORK RECOVERY TIME*) : métrique déterminant le temps maximum tolérable nécessaire pour vérifier l'intégrité du système et/ou des données.

RESSOURCES UTILES

GÉNÉRAL

ANSSI

- *Attaques par rançongiciels, tous concernés comment les anticiper et réagir en cas d'incident ?*, 2020 : www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident
- *État de la menace rançongiciel à l'encontre des entreprises et institutions*, 2020 : www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001
- Les guides techniques et les recueils de bonnes pratiques : www.ssi.gouv.fr/administration/bonnes-pratiques/
- Produits et services qualifiés par l'ANSSI : www.ssi.gouv.fr/entreprise/qualifications/produits-recommandes-par-lanssi/les-produits/
- « Ne soyez plus otage des rançongiciels » : www.ssi.gouv.fr/actualite/ne-soyez-plus-otage-des-rancongiciels/
- Site du CERT-FR www.cert.ssi.gouv.fr/cti

CYBERMALVEILLANCE.GOUV.FR

Fiche réflexe « Que faire en cas d'attaque par rançongiciel » : www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

FICHE 1

ANSSI

- *Cartographie du système d'information, guide l'élaboration en 5 étapes,* 2018 : www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/
- *Méthode EBIOS Risk Manager,* 2018 : www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager

FICHE 2

ANSSI

- *Cartographie du système d'information, guide l'élaboration en 5 étapes,* 2018 : www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/
- *Guide d'hygiène informatique*, 2017 : www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
- *Maîtrise du risque, l'atout confiance*, 2019 : www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/
- *Méthode EBIOS Risk Manager,* 2018 : www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager
- Points de contrôle Active Directory, 2020 : www.cert.ssi.gouv.fr/uploads/guide-ad.html
- *Recommandations de sécurité relatives à l'Active Directory*, 2014 : www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

AFNOR

- *ISO 22301:2019 Sécurité et résilience, Systèmes de management de la continuité d'activité*, 2019 : www.iso.org
- *ISO 22320:2018 Sécurité et résilience, Gestion des urgences, Lignes directrices pour la gestion des incidents,* 2018 : www.iso.org
- *ISO/IEC 27035-1:2016 Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information — Partie 1 : Principes de la gestion des incidents,* 2016 : www.iso.org

SGDSN

- *Guide pour réaliser un plan de continuité d'activité, 2013 :* www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

FICHE 6

AMRAE

- *Maîtrise du risque,* « Étape 6 : mettre en place des polices d'assurance adaptées », 2019 : www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/ (p. 28)

FICHE 7

ANSSI

- *Organiser un exercice de gestion de crise cyber, 2020 :*
  www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/

FICHE 11

ANSSI

- Déclarer un incident sur le site de l'ANSSI :
  www.ssi.gouv.fr/en-cas-dincident

CNIL

- Notifier une violation de données personnelles.
  www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

CYBERMALVEILLANCE.GOUV.FR

- Assistance en cas d'incident :
  www.cybermalveillance.gouv.fr/diagnostic

FICHE 14

COLLECTIF NOMORERANSOM

- www.nomoreransom.org/fr/

COLLECTION
GESTION DE CRISE CYBER

« Pour assurer leur résilience, les organisations doivent se dire que leurs efforts en cybersécurité ne suffisent pas toujours… Et bel et bien se préparer à la possibilité d'une attaque ! On ne peut en effet pas improviser des réponses en plein milieu d'une catastrophe. La préparation, l'outillage et l'entraînement des experts cyber et des métiers sont indispensables pour maintenir l'activité en cas d'attaque informatique… »

Guillaume Poupard, directeur général de l'ANSSI

Se préparer, côté métiers comme côté technique, à gérer les effets d'une crise d'origine cyber est aujourd'hui primordial pour gagner en résilience.

Réalisé en partenariat avec le Club des directeurs de sécurité des entreprises et fruit d'une riche expérience dans la gestion de crise cyber, ce guide vous accompagnera dans la mise en place d'outils et de procédures de crise efficients et résilients.

Version 1.0 – Décembre 2021 – **ANSSI-PA-089**

ISBN : 978-2-11-167108-9 (papier)
ISBN : 978-2-11-167109-6 (numérique)
Dépôt légal : décembre 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr