MEDIA CONTACT
The offshore company

GESTION DE CRISE AUTOUR DES DONNEES PERSONNELLES (FUITE, CYBERATTAQUE, ETC.)

Revision History	
Last updated	Janvier 2021

GROUPE MEDIA CONTACT SA

Avenue Dorothée LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

+229 **95 17 00 16**
contact@groupmediacontact.com

RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Sommaires

I. INTRODUCTION

Le monde actuel est en train de vivre une révolution numérique. Les nouvelles technologies (et en particulier celles liées à l'informatique et aux télécommunications) sont en train de bouleverser le monde des entreprises. Cette révolution numérique a donc également des répercutions sur la sécurité des entreprises. Leur niveau d'exposition aux risques en général et aux risques cyber en particulier est depuis quelques années en perpétuelle augmentation et est devenu un sujet d'attention et de préoccupation pour les dirigeants des entreprises. La mondialisation et la numérisation du monde des affaires et des échanges commerciaux ont fait apparaître de nouvelles sources et de nouveaux types de menaces. Les Systèmes d'Information (SI) des entreprises hébergent une multitude d'informations qui attirent la convoitise, que ce soit de la part de compétiteurs, de cyber-délinquants, voire même de personnes internes à la société. Ces mêmes systèmes d'information sont de plus en plus interconnectés et ouverts (par exemple sur Internet), et offrent donc une exposition de plus en plus large aux intrusions et aux attaques qui peuvent être initiées depuis n'importe quelle partie du monde.

Il convient d'abord de rappeler la définition d'une « crise »: « Événement soudain causant des pertes et des dommages importants, entraînant une interruption d'une ou plusieurs activités critiques ou un arrêt de l'organisme, ayant des impacts à long terme et nécessitant le recours à la Cellule de crise et, le cas échéant, à un site alternatif. Une crise peut avoir des conséquences sur la survie même de l'entreprise.» Par conséquent, la crise est une résultante de la matérialisation de risque(s) ayant des impacts non maîtrisables pouvant mettre en péril la réputation, les opérations, voire la pérennité même, de l'entreprise ou de la structure qui la subit. En règle générale, la crise est imprévisible, et lorsqu'elle se matérialise, elle est généralement source de désorganisation et l'entreprise qui en est victime

doit être en mesure de fournir immédiatement des réponses adaptées et justement calibrées en fonction de la typologie de celle-ci.

II. LES SPECIFICITES D'UNE GESTION DE CRISE CYBER

La gestion de crise cyber doit être pluridisciplinaire : elle est notamment au croisement de la gestion du risque et de la sécurité informatique (donc technique). Les experts techniques seront au service du décisionnaire dans cette gestion. Une particularité des crises cyber est que l'attaque, en altérant le SI de l'entreprise, peut directement diminuer sa capacité de réponse. Il convient donc de disposer d'un dispositif de gestion de crise qui permette de pallier à cette possibilité et par conséquent :

- Prévoir des moyens de gestion de crise hors SI ;
- Se doter de postes de travail durcis hors des domaines d'administration ;
- D'exploiter des services d'échange et de communication externes (par exemple des services cloud).

III. DISPOSITIF DE GESTION DE CRISE A MEDIA CONTACT

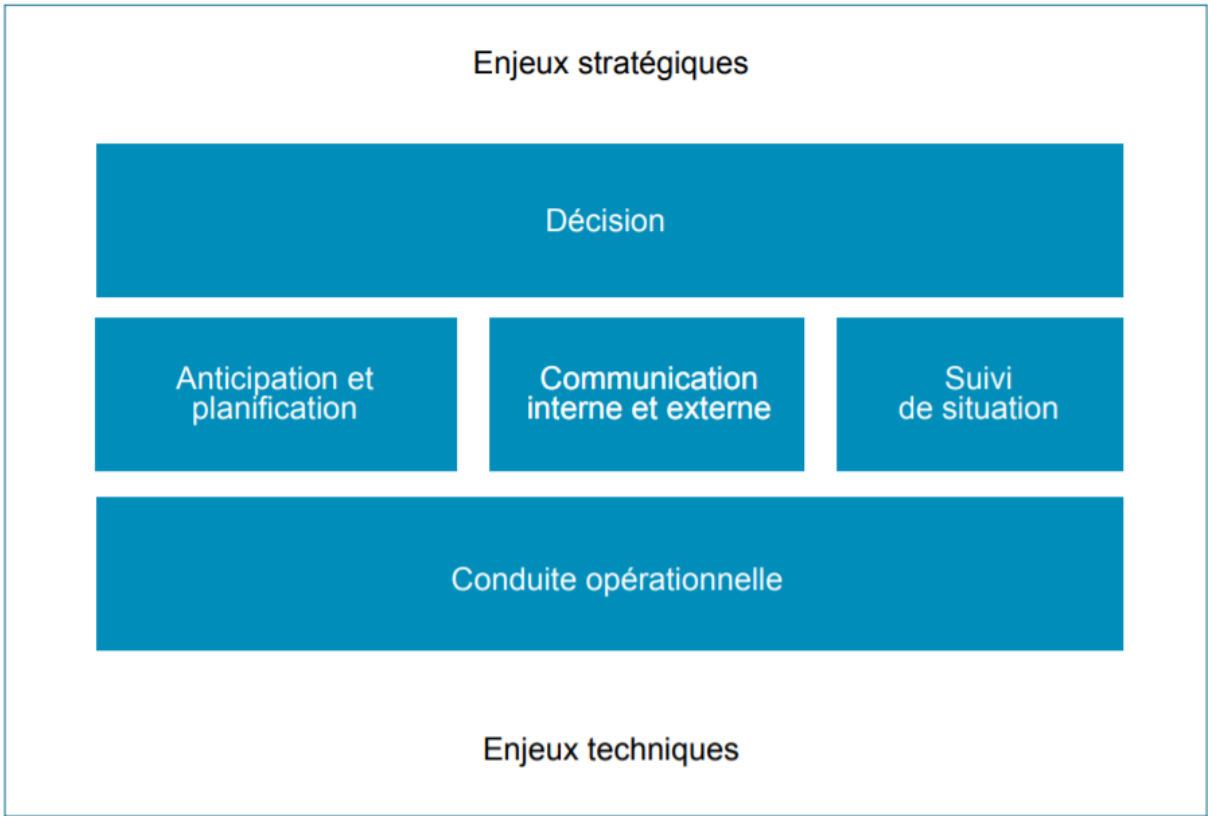
L'organisation de la gestion de crise au sein de MEDIA CONTACT respecte certains principes parmi lesquels on peut citer :

1. Un pilotage stratégique, assuré par la tête de l'entité. La fuite de données n'étant pas seulement une crise informatique, le pilotage sera assuré par la Direction Générale, Directeur sécurité et (secrétaire

général) …, qui fera la synthèse entre la vision business et les réalités techniques. L'implication du top management est ainsi l'une des conditions essentielles de l'efficacité du dispositif ;

2. Une conduite opérationnelle assurée par le ou les métiers impliqués. ;
3. La mobilisation d'experts internes ou externes (si nécessaire) qui apporteront un éclairage complémentaire et un certain recul sur la situation. Les experts externes pourront aussi constituer des alliés précieux en matière de communication ;
4. Une veille et un suivi de situation permanents.

Schéma : les fonctions d'un dispositif de gestion de crise



IV. LES GRANDES ETAPES DE LA GESTION DE CRISE A MEDIA CONTACT

Etape 1 : l'alerte.

- Un lanceur d'alerte signale une fuite de données directement à l'organisation ce qui appelle une réponse rapide de façon à éviter que l'information ne se propage dans la presse ;
- Un hacker signale lui-même la fuite à l'entreprise. Là aussi, l'information devra être rapidement prise en compte avec toutes les précautions nécessaires.
- L'equipe sécurité de l'entreprise détecte un incident et transmet l'alerte à sa hiérarchie après une première évaluation. Dans le cas d'un chantage, s'il faut maintenir un canal de discussion pour gagner du temps.

Etape 2 : l'escalade et la mobilisation.

Une évaluation plus approfondie est menée pour savoir s'il y a lieu de mobiliser le dispositif de crise. Tout incident ne constitue pas forcément une crise potentielle. Dans le cas d'une fuite de données, il s'agira d'évaluer l'impact en termes de confidentialité et d'intégrité des données, en s'appuyant sur les analyses d'impact (Privacy Impact Assessment ou PIA) qui ont normalement été réalisées pour chaque traitement de données personnelles. Si l'incident est considéré comme suffisamment grave sur la base de différents critères (périmètre de la fuite, nature des données « fuitées », risque juridique, risque financier, impact en termes d'image…), le dispositif de crise est alors immédiatement activé.

Etape 3 : le confinement

L'objectif est de prendre les mesures d'urgence permettant de faire cesser la fuite de données, par exemple en mettant en suspens le traitement de données incriminé. Une étape particulièrement délicate puisqu'il s'agira souvent de faire des arbitrages entre la volonté d'isoler, voire de couper, telle ou telle partie du système d'information, et le besoin de maintenir en l'état ce même système pour permettre les investigations futures. L'arrêt d'un serveur peut en effet avoir pour conséquence de détruire les données stockées en mémoire vive, tandis qu'une déconnexion du réseau diminuera les chances de remonter jusqu'à un éventuel attaquant.

Etape 4 : les investigations techniques.

Cette étape est primordiale, tant d'un point de vue opérationnel afin de comprendre les causes de la fuite de donnée et y remédier, qu'au plan juridique et assurantiel. Elle donne lieu à l'exploitation, par une équipe interne ou externe, de l'ensemble des logs de connexion.

Etape 5 : la notification aux autorités.

La notification à la CNIL par le responsable de traitement, qui peut se faire en quelque lignes , doit avoir lieu au plus tard dans les 72 heures après que l'organisation a eu connaissance de la fuite. La CNIL peut d'ailleurs avoir été prévenue simultanément par le lanceur d'alerte, ce qui renforce la nécessité de réagir rapidement. La notification devra être assurée en parallèle auprès de l'ANSSI.

Etape 6 : la notification aux clients.

Dès lors que la fuite entraine « un risque élevé pour les droits et libertés d'une personne physique » le responsable du traitement doit notifier aux les clients concernés dans les meilleurs délais. A noter qu'il existe quelques dérogations, notamment dans le cas où les données fuitées ne sont pas exploitables, par exemple lorsqu'elles sont chiffrées.

Etape 7 : la remédiation et la restauration.

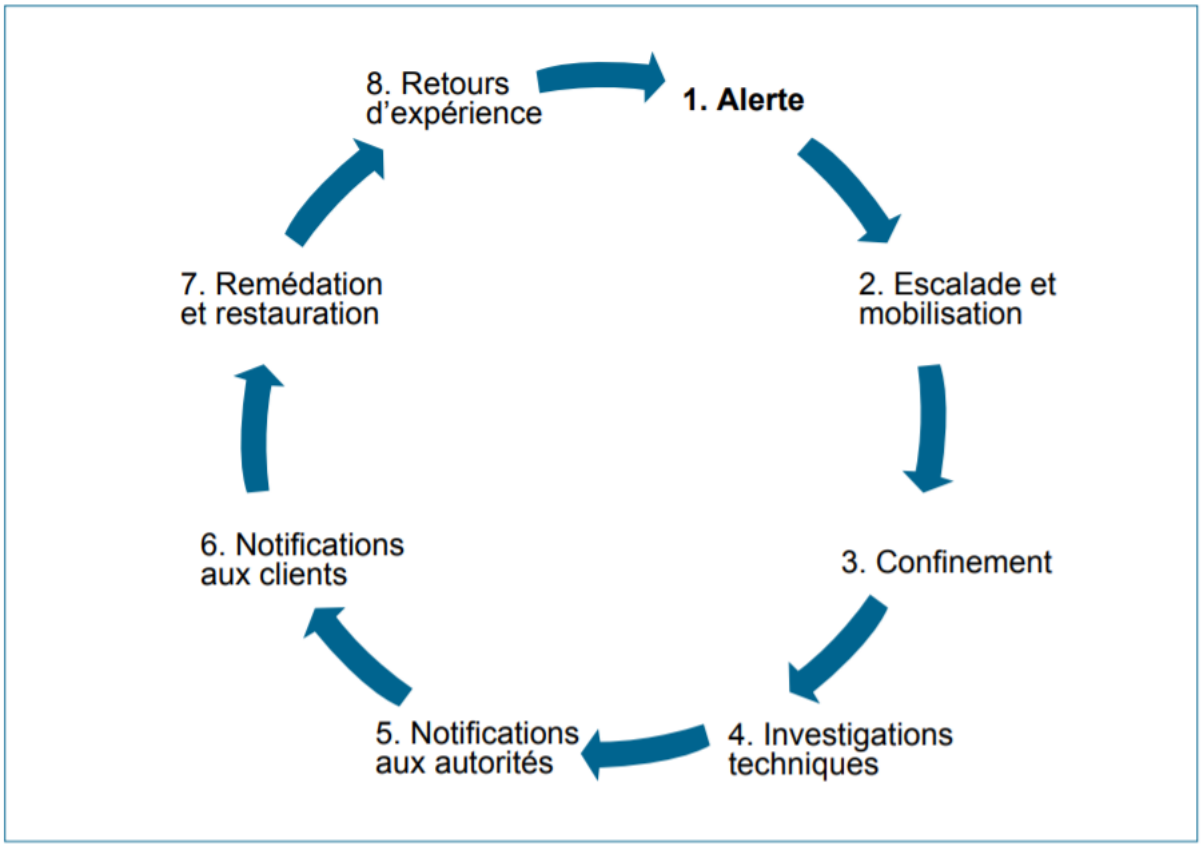
Il est bien sûr préférable que cette étape ait lieu une fois les causes techniques de l'incident identifiées et analysées.

Etape 8 : le retour d'expérience.

Toute crise doit donner lieu à un retour d'expérience (RETEX) permettant d'améliorer le dispositif. Ce RETEX concerne à la fois le renforcement des capacités de détection, par exemple par l'intégration de nouvelles règles techniques, la création d'un « set » de réponses à incident plus ou moins automatisées, et la recherche d'une meilleure application de la politique de sécurité des systèmes d'information, notamment en matière de mise à jour des serveurs critiques. Ce processus vise aussi à améliorer le fonctionnement d'ensemble du dispositif par l'optimisation des procédures et moyens mis à disposition.

.

Schéma : les étapes de la gestion de crise



V. LES MOYENS MISE A DISPOSITION DE L'EQUIPE DE GESTION DE CRISE

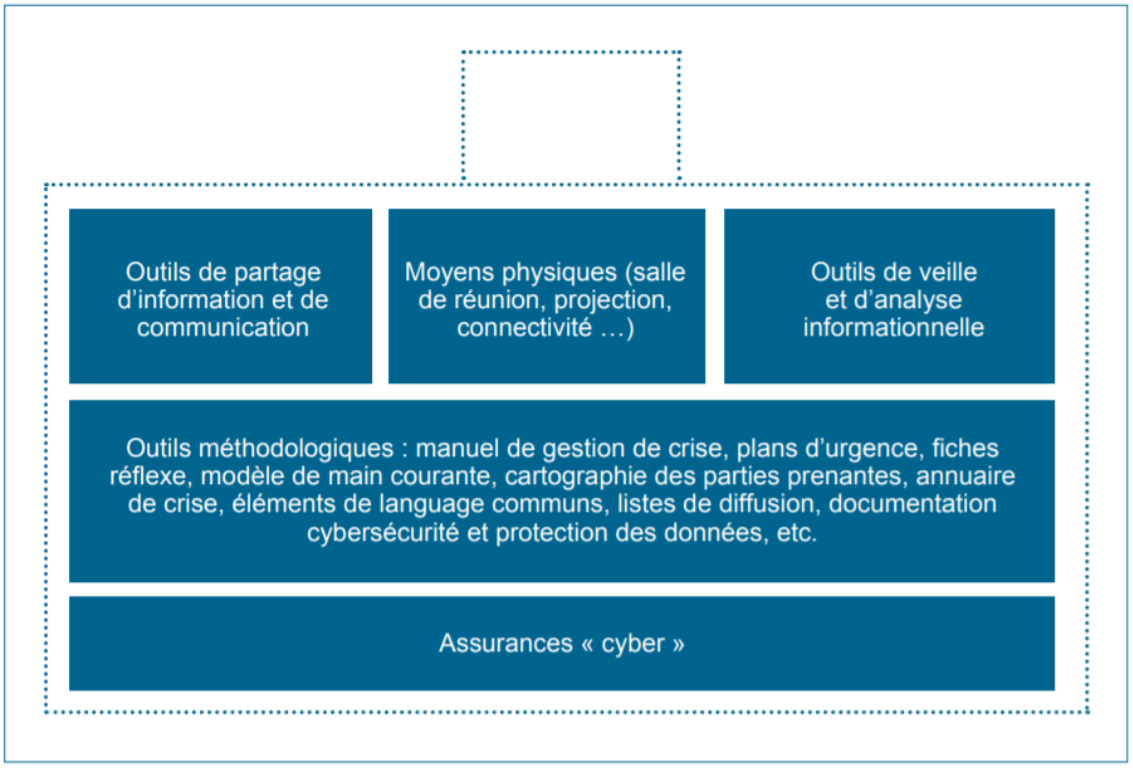
La compression du temps en situation de crise exige la mobilisation rapide d'une boîte à outils testée au préalable. Elle est composée :

- D'outils de partage d'information et de communication : mise en place d'un espace documentaire, d'une messagerie instantanée.
- De moyens physiques : Une ou plusieurs salles de réunion est mis à disposition du dispositif de crise avec l'ensemble des capacités nécessaires (connectivité, projection…).
- De capacités de veille informationnelle : Indépendamment des capacités de surveillance et de détection utilisées en amont pour

détecter au plus tôt la survenance d'une fuite de données, une veille spécifique, en temps réel, est menée, en particulier sur les réseaux sociaux, pour suivre les retombées de la crise et alimenter la tenue de « situation opérationnelle ».

- D'outils méthodologiques : Outre le manuel de gestion de crise et l'ensemble des plans d'urgence (PCA/PRA, etc.), il s'agit aussi de disposer de quelques outils génériques : annuaire de crise interne et externe, listes de diffusion interne et externe.
- D'assurances spécifiques. Si les assurances traditionnelles couvrent les dommages matériels sur les réseaux et systèmes d'information, les polices d'assurance spécifiquement « cyber » permettent d'assurer les conséquences liées aux atteintes aux données.

Schéma : la boîte à outils de la gestion de crise



VI. Nos principes de communication en période de crise

- Préparer des éléments de langage factuels sur le dispositif de cybersécurité et de protection des données personnelles et sur les valeurs de l'entreprise. Faute d'éléments précis sur les causes techniques de la fuite de données lors des premiers jours suivant le déclenchement de la crise, son périmètre ou les victimes potentielles.
- Désigner un porte-parole au sein de l'organisation. Ce porte-parole pourra être assisté d'un expert SI ou cybersécurité qui utilisera des canaux de communication plus techniques (réseaux sociaux notamment).
- Prendre l'initiative et communiquer régulièrement tout au long de la crise sans attendre systématiquement que l'information ne parvienne à la presse et ne conduise l'organisation à agir sur un mode exclusivement réactif.
- S'appuyer sur une parfaite identification des parties prenantes (clients, fournisseurs, autorités, associations, médias, élus…) afin de préparer des messages ciblés et d'identifier les canaux de communication les plus appropriés.
- Être transparent. Toute information ne doit pas être nécessairement communiquée mais celle qui est diffusée doit être authentique et vérifiable.
- Éviter le rétropédalage en donnant des informations non vérifiées. Rien n'est pire que de revenir sur ses propres déclarations pour « rectifier le tir », par exemple sur le nombre de victimes potentielles.
- Rester simple dans ses explications en s'appuyant sur des exemples et des cas concrets.
- Ne pas chercher à se défausser ou à rejeter sa responsabilité sur un tiers. Cette attribution est non seulement techniquement délicate, voire impossible, mais stratégiquement maladroite. La mise en cause

publique d'un sous-traitant devra ainsi être évitée.

- Établir un canal de communication direct avec ses clients (numéro vert, forum…). La communication ne peut pas être unidirectionnelle.
- Gérer en parallèle la communication interne et impliquer l'ensemble des salariés lors de la sortie de crise pour faire de celle-ci un élément de mobilisation et éviter la frustration, assez fréquente, des salariés qui apprennent par l'extérieur une information concernant leur propre organisation.