ceis

DÉCEMBRE 2018

FUITE DE DONNÉES : GESTION DE CRISE, MODE D'EMPLOI

Par Guillaume Tissier, CEIS

Les notes stratégiques

L'INTELLIGENCE DE LA DÉCISION

LES NOTES STRATÉGIQUES

Notes d'étude et d'analyse

TABLE DES MATIÈRES

INTRODUCTION

« Ce qui ne me tue pas me rend plus fort ».

Friederich Nietsche

1 000 violations de données personnelles ont été déclarées auprès de la CNIL depuis le 25 mai 2018, date de l'entrée en vigueur du Règlement européen sur la protection des données personnelles (RGPD), résultant pour moitié d'attaques, pour moitié de négligences ou d'erreurs. Et aucun secteur n'est à l'abri : si ceux de la restauration et de l'hôtellerie sont surreprésentés en raison de la fuite ayant affecté en juin 2018 Fastbooking[1], une plateforme de réservation en ligne, les services financiers et les assurances, le e-commerce ou l'industrie, sont également touchés.

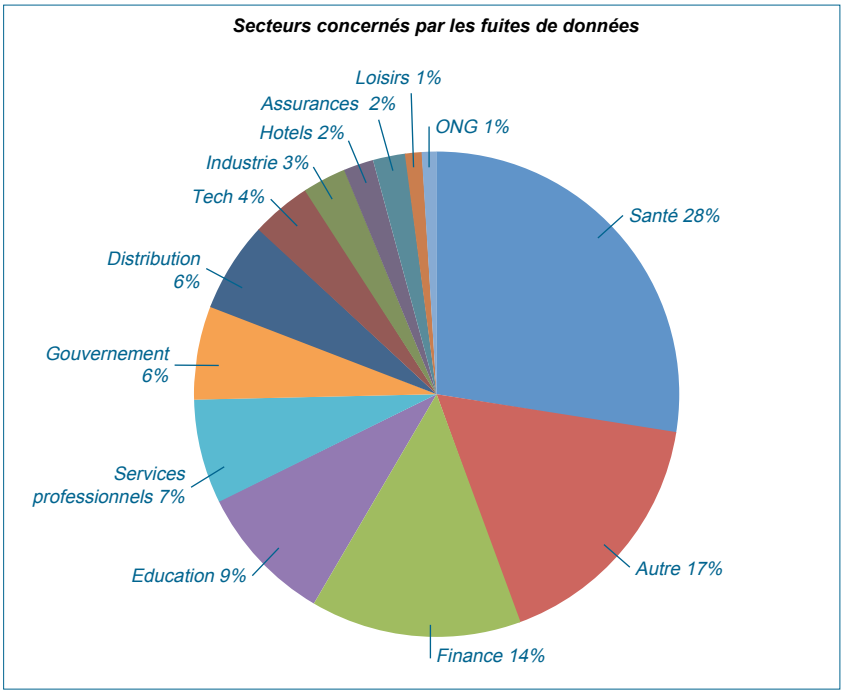
Face à ces hémorragies de données, l'élaboration et la mise en œuvre de **stratégies de prévention et de protection** visant à durcir et à intégrer « by design » la sécurité des réseaux et des systèmes d'information et la protection des données personnelles sont essentielles. A l'heure de « l'entreprise étendue » et du *big data*, le concept de « **zero trust architecture** », qui consiste à toujours vérifier et à ne jamais faire confiance, s'impose. Parce qu'il n'est plus possible de distinguer l'intérieur de l'organisation de l'extérieur, tous les utilisateurs et les flux doivent par défaut être suspects.

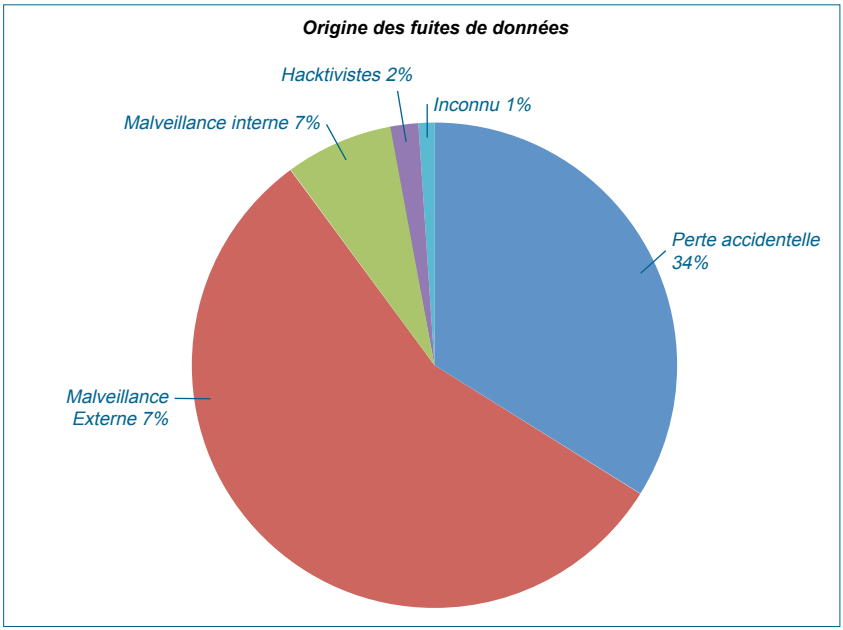
Au risque de décevoir, ces réponses, même si elles sont indispensables, ne suffisent pas. Toutes les organisations, même les plus matures, seront tôt ou tard victimes d'une fuite de données en raison de la croissance exponentielle de leur surface d'exposition, de la multiplication et de la sophistication des menaces, et de l'instrumentalisation des fuites de données comme outil de déstabilisation à l'encontre des États et des entreprises. **La question n'est donc plus de savoir « si » mais « quand » cette fuite aura lieu, et de s'y préparer.**

Les fuites de données sont en effet des crises « à part ». Forte viralité, multiplicité des parties prenantes (clients, prestataires, autorités, société civile…), déconnexion entre la réalité technique de la crise et la perception du grand public, conséquences en termes d'image de marque, responsabilités multiples en raison du recours fréquent à de nombreux sous-traitants, judiciarisation croissante etc. : tout concourt à faire naitre chez l'entreprise, qu'elle soit coupable, victime, ou bien les deux à la fois, un **sentiment d'impuissance et d'incompréhension** que seule une préparation minutieuse en amont permettra de compenser.

---

[1] *Les seuls chiffres communiqués sont issus du marché japonais, où 380 établissements auraient été touchés et les données bancaires de 124 963 clients auraient été dérobées.*





Source : Breach Level Index, données premier semestre 2018 [2].

LES 10 CARACTÉRISTIQUES CLÉS D'UNE FUITE DE DONNÉES

Chaque crise possède des caractéristiques propres et il en va de même pour les fuites de données. On peut toutefois distinguer certaines caractéristiques communes :

1. Ce sont des crises globales. Les crises cyber ou impliquant une dimension cyber ne sont pas de simples crises techniques, IT ou SSI. Leur impact est d'abord « business ».

2. Elles exigent une approche pluridisciplinaire. Les fuites de données exigent une réponse globale associant une réaction technique à des réponses « métier », juridique, assurantielle etc. La plupart des fonctions de l'organisation doivent donc être impliquées dans le dispositif, au premier rang desquels la direction générale.

3. Ce sont des crises imprévisibles. Même si les capacités d'anticipation et de détection s'améliorent, l'asymétrie traditionnelle entre attaquant et défenseur rend les fuites d'origine malveillante difficiles à prévoir.

4. Ces crises ont une temporalité différente. Contrairement à des crises traditionnelles dont les effets sont généralement limités dans le temps ou qui obéissent à des règles de propagation à peu près établies, les crises cyber ne se soumettent à aucune règle. La fuite peut être découverte plusieurs mois après l'intrusion dans le système d'information et produire des effets encore plusieurs mois après.

5. Elles placent les organisations victimes dans une situation de « sous-information » chronique, débouchant sur un fort sentiment d'impuissance. La nature technique de l'environnement numérique, le « brouillard » qui l'entoure, la multiplicité des causes et la durée des investigations techniques expliquent que les organisations mettent longtemps à identifier les causes réelles de la crise, ce qui complexifie leurs actions de communication. Les organisations étendues et le recours à des sous-traitants multiples qui opèrent des infrastructures (IaaS), des plateformes (PaaS), des services (SaaS), voire des processus « business » complets (BpaaS) compliquent encore les choses, ce qui exige sur le plan juridique une délimitation claire des responsabilités entre le responsable de traitement et le sous-traitant.

---

[2] *https://breachlevelindex.com/data-breach-library*

6. Ces crises ont une viralité importante. Les fuites de données sont très médiatisées et bénéficient d'une forte viralité en raison de la sensibilité croissante des utilisateurs à la protection de leurs données. Au point qu'il y a parfois un véritable décalage entre la réalité de la crise et sa perception par les acteurs externes en raison de la brutale rupture de confiance qu'elle génère et de la curiosité qu'elle suscite auprès du public. L'organisation, même victime, sera considérée comme co-responsable, voire coupable : elle ne pourra donc pas espérer rester « en dessous du radar » et sera contrainte de s'exprimer en ayant à l'esprit que la perception compte souvent plus que la réalité…

7. Leurs impacts sont difficiles à évaluer. Les crises cyber sont des crises systémiques avec des effets multiples, en cascade, et non limitées géographiquement. Point clé : les impacts « métiers » se traduisent nécessairement en pertes financières et en atteintes à l'image de marque, plus difficilement quantifiables mais bien réelles, d'autant que le public aura besoin d'identifier un responsable, peu importe les circonstances de la fuite de données. La confiance se gagne dans la durée mais se perd en quelques minutes…

8. Elles font l'objet d'une judiciarisation croissante. La sensibilité croissante de la société civile à la protection des données personnelles et l'émergence de cadres législatifs et réglementaires en matière de protection des données débouchent sur une judiciarisation croissante des fuites de données, et la nécessité pour les organisations de mettre en place, en amont, une approche de conformité.

9. Elles nécessitent des arbitrages complexes entre continuité et réponse juridique. Le besoin de geler la « scène de crime » pour les investigations, préalable indispensable à toute action judiciaire et à la mise en œuvre d'une éventuelle police d'assurance, se heurte souvent à la volonté des organisations de faire redémarrer au plus vite leurs activités pour limiter l'impact de la crise.

10. Elles affaiblissent les capacités de réponse des organisations. L'impact de la crise sur le système d'information et la mise en œuvre de mesures conservatoires entravent souvent les capacités de réponse et de continuité des organisations. Difficile, par exemple, de mettre en œuvre une communication vers les clients lorsque les canaux de communication traditionnels ont été coupés ou lorsqu'une partie des systèmes d'information est momentanément paralysée.

Les spécificités des crises résultant de fuites de données impliquent donc **d'adapter le dispositif de gestion de crise existant.** Il s'agira, au-delà des capacités de prévention destinées à réduire ses vulnérabilités et sa surface d'exposition aux risques, et des capacités de détection qui permettront d'identifier le plus en amont possible un incident susceptible de déboucher sur une crise, de travailler à la fois sur l'**organisation, les moyens et les processus de gestion de crise** pour réduire son impact lorsque qu'elle n'aura pu être empêchée.

QUEL DISPOSITIF DE GESTION DE CRISE ?

L'organisation de la gestion de crise doit bien sûr être adaptée à chaque entité mais certains principes devront être respectés :

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, un membre du COMEX ou l'un de ses représentants (secrétaire général, *risk manager*, directeur sécurité/sûreté…), qui devra faire 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. Ce pilotage devra par ailleurs permettre à l'entité de se positionner à la fois dans une posture de « temps court » et de « temps long » pour anticiper le « coup d'après ». Objectif : ne plus subir la crise et reprendre la main.

2. L'implication de toutes les fonctions transverses. Le pilotage stratégique devra associer toutes les fonctions transverses susceptibles d'être impliquées dans la crise, qu'il s'agisse de la DSI, du RSSI, de la direction juridique, du DPO, du *risk manager,* de la direction de la communication interne et externe, voire des directions de la conformité et des affaires publiques pour les organisations en disposant.

3. Une conduite opérationnelle assurée par le ou les métiers impliqués. « Le terrain commande », dit-on dans les Armées. De fait, si le pilotage global de la crise ne doit pas leur incomber, ce seront le ou les métiers impliqués qui auront la main sur la conduite opérationnelle, tout en étant appuyés par les directions transverses.

4. La mobilisation d'experts internes ou externes 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. Si l'entreprise ne dispose pas de service juridique, il sera également essentiel de s'appuyer sur les services d'un avocat spécialisé, ne serait-ce que pour les éventuelles suites judiciaires.

5. Une veille et un suivi de situation permanents. La *situational awareness* permet une bonne appréciation de la situation, et facilite donc la prise de décision. Ce processus fonctionnera à la manière d'une gare de triage de l'information et se traduira par l'organisation de points de situation réguliers et la tenue d'une main courante qui permettra d'enregistrer tout événement, information externe et prise de décision, tant pour des raisons juridiques et assurantielles (prouver que l'organisation a bien mis en œuvre telle ou telle mesure) que pour faciliter le retour d'expérience post-crise.

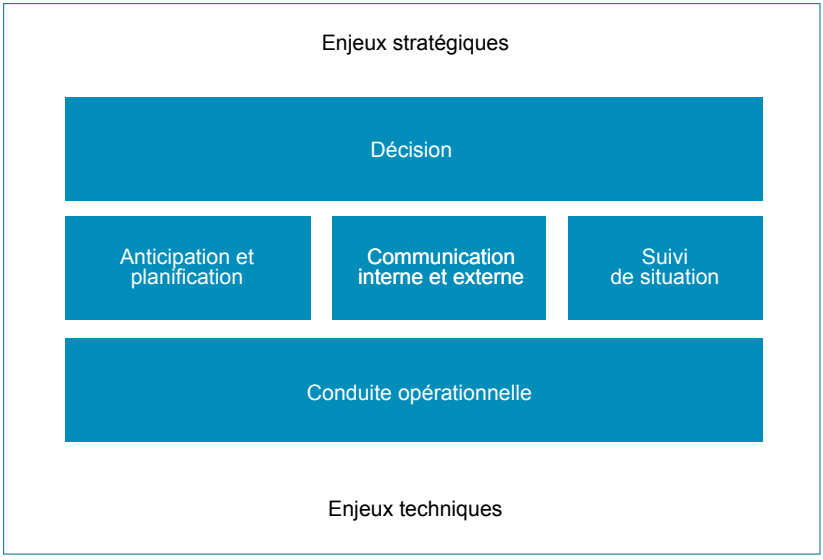
POINT CLÉ : L'ARTICULATION ENTRE LES NIVEAUX STRATÉGIQUES ET OPÉRATIONNELS

Dans les grandes organisations, l'échelon opérationnel pourra faire l'objet d'une cellule spécifique, dont le fonctionnement devra être soigneusement articulé avec une cellule « tête de groupe », très resserrée, assurant le pilotage stratégique de la crise et réunissant les grandes fonctions transverses. Une autonomie excessive de la cellule opérationnelle, fréquente lorsque les deux cellules sont éloignées géographiquement, tout comme une mainmise de la cellule stratégique sur les opérations et un micro-management de la crise devront être évitées. Inutile par exemple d'épuiser la cellule opérationnelle par des demandes permanentes de comptes-rendus. Il est essentiel de ménager les hommes, les crises s'installant parfois dans la durée…

De façon globale, le dispositif mis en place pour traiter des fuites de données devra ainsi couvrir les fonctions génériques suivantes : **la prise de décision, l'anticipation et la planification, le suivi de situation, la conduite opérationnelle, la communication interne et externe.** L'utilisation d'une matrice RACI[3] permettra d'attribuer des rôles et de déterminer les périmètres de responsabilité entre les différents acteurs. Au plan RH, il pourra enfin être utile de prévoir un fonctionnement 24/7, avec toutes les incidences contractuelles que cela peut avoir en interne et sur les sous-traitants.

Pour être efficace, ce dispositif devra impérativement avoir été **mis en place en amont et maintenu en condition opérationnelle** grâce à des campagnes de sensibilisation régulières, des exercices stratégiques (ou table-top) et des entrainements opérationnels pour les équipes techniques. Objectif : favoriser des actes-réflexe et éviter toute improvisation en situation réelle. Des *media training* pourront aussi être organisés pour les porte-paroles qui seront désignés.

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



[3] *La matrice RACI (« Responsible, Accountable, Consulted, Informated ») permet de visualiser facilement la répartition des rôles sur un projet donné.*

QUELLES SONT LES GRANDES ÉTAPES DE LA GESTION DE CRISE ?

ETAPE 1 : L'ALERTE.

Elle peut avoir 3 origines :

1. Un lanceur d'alerte signale une fuite de données directement à l'organisation (exemple : le protocole utilisé par le site Zataz[4] destiné à avertir les organisations d'une vulnérabilité, d'une fuite ou d'un piratage), ce qui appelle une réponse rapide de façon à éviter que l'information ne se propage dans la presse ;

2. 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, *a fortiori* si le hacker n'est pas « éthique » et tente de monnayer sa découverte, voire de faire chanter l'organisation ;

3. Le SOC/CERT de l'entreprise, internalisé ou externalisé, 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, il est formellement déconseillé de payer. Rien ne garantit que le pirate ne divulguera pas les données collectées après le paiement, et cela accréditera en plus l'idée que l'entreprise est responsable de la situation.

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 (cf. article 35 du RGPD). 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.

---

[4] *https://www.zataz.com/protocole-alerte-zataz/*

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 et à un travail de *hunting* interne pour détecter d'éventuelles APT sur le réseau. A noter de ce point de vue l'importance des systèmes de « bastion » qui permettent d'enregistrer et de surveiller l'ensemble des accès aux serveurs et données critiques de l'entreprise.

ETAPE 5 : LA NOTIFICATION AUX AUTORITÉS.

En vertu de l'article 33 du RGPD, la notification à la CNIL par le responsable de traitement, qui peut se faire en ligne[5], 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. A noter que pour les Opérateurs d'Infrastructures Vitales (OIV) ou Opérateurs de Services Essentiels (OSE) au sens de la directive NIS, 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 » (article 34 du RGPD), le responsable du traitement doit notifier 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[6].

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.

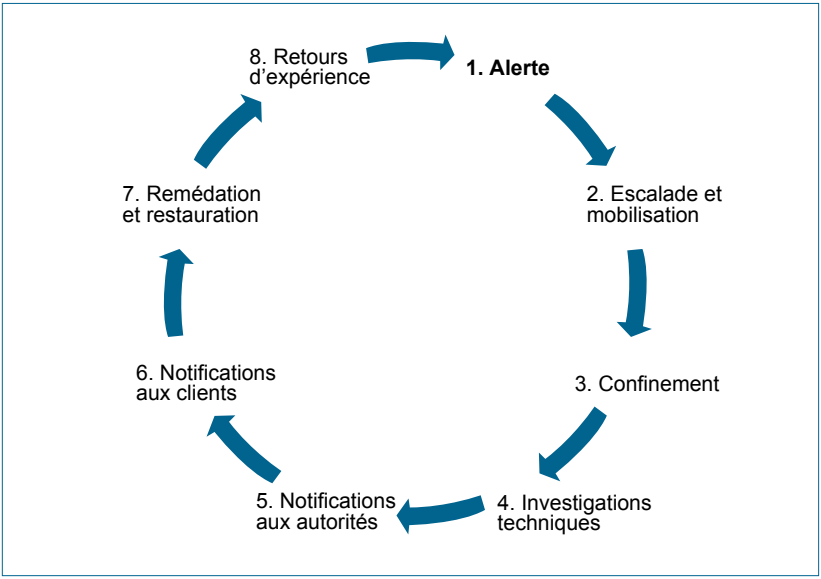
Toute crise doit donner lieu à un retour d'expérience (RETEX) permettant d'améliorer le dispositif. Ce RETEX concerne à la fois le renforcement des capacités de détection, par exemple par l'intégration de nouvelles règles techniques, la création d'un « set » de réponses à incident plus ou moins automatisées, 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 visera aussi à améliorer le fonctionnement d'ensemble du dispositif par l'optimisation des procédures et moyens mis à disposition.

---

[5] https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

[6] Selon le Breach Level Index, ce cas ne concerne cependant que 3% des fuites de données observées dans le monde pour le moment.

Schéma : les étapes de la gestion de crise



QUELLE BOÎTE À OUTILS ?

La compression du temps en situation de crise exige la mobilisation rapide d'une boîte à outils qui doit être testée et éprouvée au préalable.

ELLE EST COMPOSÉE :

1. D'outils de partage d'information et de communication, si possible distincts de l'infrastructure habituelle de l'organisation potentiellement atteinte par la crise. Exemples : mise en place d'un espace documentaire de type « data room », d'une messagerie instantanée et d'un système de téléphonie sécurisée.

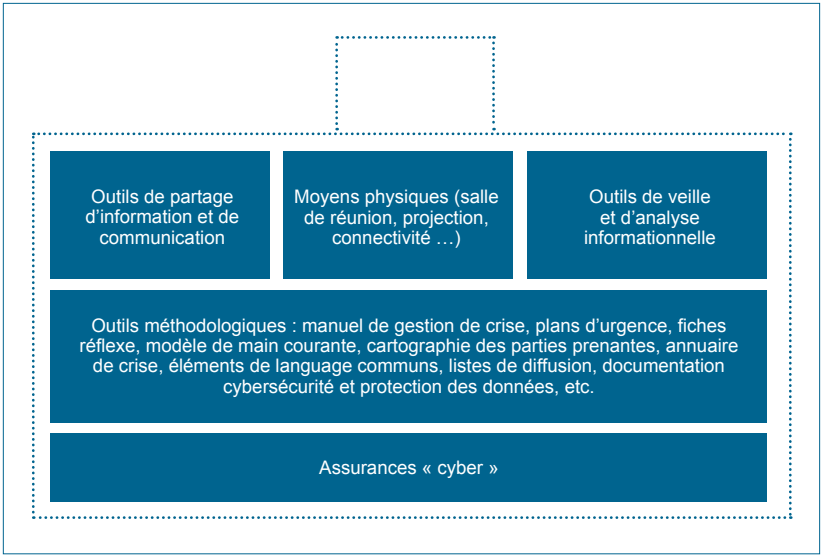
2. De moyens physiques. Une ou plusieurs salles de réunion devront être mises à disposition du dispositif de crise avec l'ensemble des capacités nécessaires (connectivité, projection…).

3. 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, devra être menée, en particulier sur les réseaux sociaux, pour suivre les retombées de la crise et alimenter la tenue de « situation opérationnelle ».

4. D'outils méthodologiques. Outre le manuel de gestion de crise et l'ensemble des plans d'urgence (PCA/PRA, etc.), il s'agira aussi de disposer de quelques outils génériques : modèle de « main courante », cartographie des parties prenantes, annuaire de crise interne et externe, listes de diffusion interne et externe… Quelques outils spécifiques aux fuites de données seront également utiles : fiche « réflexe » décrivant les différentes étapes d'une crise de ce type et les actions clés, éléments de langage commun comprenant par exemple le descriptif du dispositif RGPD et de cybersécurité, liste des traitements de données personnelles, synthèse des analyses d'impact, cartographie des sous-traitants utilisés, description de l'éventuelle police d'assurance cyber…

5. 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.** Dans le cas d'une fuite de données, elles permettront par exemple de couvrir les frais de gestion de crise et de notification aux clients qui peuvent rapidement grimper. En revanche, leur activation supposera une évaluation précise de l'impact de la fuite en termes financiers. La souscription à de telles garanties impliquera aussi en amont la mise en place d'une démarche de management des risques.

Schéma : la boîte à outils de la gestion de crise



LES 10 COMMANDEMENTS DE LA COMMUNICATION DE CRISE

1. 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, il s'agira souvent d'exploiter des données factuelles sur le dispositif RGPD de l'organisation, son engagement en matière de cybersécurité etc., au risque de paraître répétitif devant les journalistes.

2. 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).

3. 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.

4. 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. Certaines de ces parties prenantes peuvent constituer des alliés précieux.

5. Être transparent. Toute information ne doit pas être nécessairement communiquée mais celle qui est diffusée doit être authentique et vérifiable.

6. 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.

7. Rester simple dans ses explications en s'appuyant sur des exemples et des cas concrets. Le jargonnage technique doit être réservé aux cibles techniques.

8. 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, d'autant qu'au titre du RGPD, l'organisation est responsable de ses sous-traitants.

9. Établir un canal de communication direct avec ses clients (numéro vert, forum…). La communication ne peut pas être unidirectionnelle.

10. 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.

POUR ALLER PLUS LOIN

À propos de CEIS

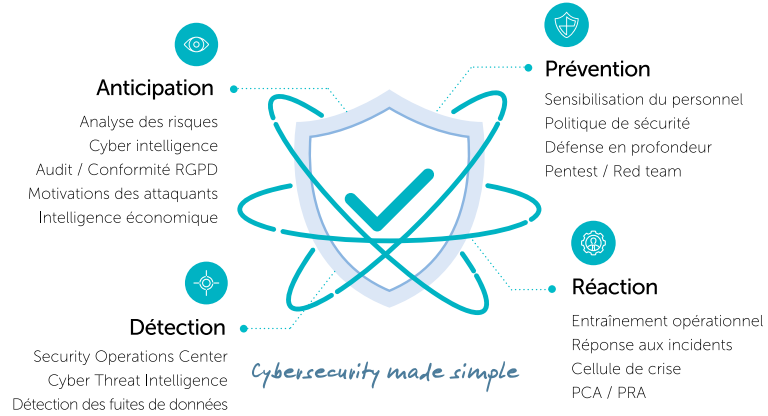
CEIS est une société de conseil spécialisée sur les questions de sécurité et de défense. Elle accompagne ses clients en matière d'intelligence économique et de cybersécurité grâce à des prestations d'investigation, de *cyber threat intelligence*, d'audit et de conseil. Elle organise également régulièrement des exercices de crise ainsi que des entrainements opérationnels dans le cadre du centre d'entrainement BlueCyForce, qu'elle anime avec Diateam.

http://www.ceis.eu

https://www.bluecyforce.com/

CEIS Cyberdefense protège les actifs sensibles de ses clients par une approche pragmatique et rationnelle, basée sur la connaissance de la menace, l'analyse des risques business et la volonté de favoriser les solutions au meilleur rapport coût/efficacité, tout en plaçant l'humain au cœur de la démarche.

L'efficacité d'un dispositif de Cybersécurité n'est pas proportionnelle au budget que l'on y consacre !



Un seul objectif : augmenter la confiance de vos clients, partenaires et investisseurs en limitant les conséquences business et métier du risque cyber.

UNE OFFRE COMPLÈTE ET INTÉGRÉE À 360°

CEIS Cyberdefense accompagne les entreprises dans la maîtrise de leurs risques cyber à travers une offre complète : stratégie et pilotage de la sécurité, anticipation des menaces et détection des fuites de données (Cyber Threat Intelligence), prévention, réponse aux incidents, assistance à la gestion de crise, détection des attaques et management de la sécurité (SOC). Cette offre est complétée par les capacités de bluecyforce, centre d'entraînement opérationnel spécialisé en cybersécurité, co-fondé par CEIS et DIATEAM, qui vise à renforcer les compétences humaines par la pratique.

ceis

PUBLICATIONS RÉCENTES

Réalité immersive, usages des réalites virtuelles et augmentées pour la Défense (Octobre 2018)
Intelligence artificielle, Applications et enjeux pour les Armées (Octobre 2018)
A2/AD, déni d'accès et interdiction de zone - Réalité opérationnelle et limites du concept (Août 2018)
Soutien des forces - Transformations d'une fonction essentielle pour les Armées (Août 2018)
Le secteur de la santé face au risque cyber : enjeux, risques, remédiations (Janvier 2018)
Sécurité des grands événements sportifs (Janvier 2018)
Blockchain : état des lieux et perspectives (Janvier 2018)

A télécharger sur **www.ceis.eu**

Compagnie Européenne d'Intelligence Stratégique (CEIS)
Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 – APE : 741 G
Tour Montparnasse – 33, avenue du Maine
BP 36 – 75 755 - Paris Cedex 15
Tél. : 01 45 55 00 20 - Fax : 01 45 55 00 60