ATTAQUE CYBER, ANTICIPER SON PLAN DE COM' AVANT LA CRISE

[LA BOÎTE À MOTS]
Communiquer en temps de crise et de transition

TABLE DES MATIÈRES

ETAPE 1

COMPRENDRE LES MENACES ET LES ENJEUX AFFÉRENTS

En matière de cybersécurité, chaque type de menace va entrainer des risques spécifiques avec des enjeux différents et des objectifs de communication bien spécifiques. C'est une réaction en chaîne. Vous devez avoir réfléchi en amont aux conséquences de chaque menace pour chaque partie prenante et aux objectifs de communication afférents.

LES ATTAQUES SUR LES DONNÉES

Les attaques visant les données constituent l'une des principales menaces pesant sur les organisations, en particulier dans un contexte de dépendance accrue aux systèmes numériques et de renforcement des exigences réglementaires (RGPD, DORA, NIS2…). Elles ciblent directement l'actif informationnel des entités, qu'il s'agisse de données personnelles, de secrets d'affaires ou d'informations stratégiques.
Ces attaques prennent des formes variées, allant du phishing de masse à des campagnes ciblées de type spear phishing ou whaling, jusqu'à l'exfiltration massive de données (data breach). Chacune d'elles soulève des enjeux spécifiques : notification obligatoire aux autorités, obligation d'information des personnes concernées, atteinte potentielle à la réputation, voire risques juridiques et contentieux.

Exemples d'attaque de données :

- **Le phishing** I Usurpation d'identité pour obtenir des données sensibles par email, SMS ou faux site.
- **Le Spear phishing** I Phishing ciblé sur une personne ou une organisation spécifique.
- **Le whaling** I Phishing ciblant des cadres dirigeants.
- **Le vol de données** I Extraction illégale de données personnelles ou stratégiques.
- **La data breach** I Fuite massive de données, souvent à la suite d'une intrusion.

LES ATTAQUES PAR LOGICIEL MALVEILLANT (MALWARES)

Parmi les différentes menaces cyber, les logiciels malveillants — ou malwares — représentent une catégorie répandue qui est à la fois évolutive et polymorphe. Leur mode opératoire et leurs conséquences opérationnelles varient considérablement, mais tous partagent un objectif commun : porter atteinte à l'intégrité, à la confidentialité ou à la disponibilité des systèmes d'information.

Chaque type de malware induit des risques spécifiques (altération des données, indisponibilité des services, perte de confidentialité, etc.), auxquels correspondent des enjeux de communication différenciés. Anticiper ces scenarii permet de structurer une réponse calibrée, en tenant compte des parties prenantes concernées, de leur niveau d'exposition, et des messages adaptés à chaque situation.

Quelques exemples de malewares:

- **Un virus** I C'est un code qui s'attache à un fichier et se propage à d'autres fichiers ou systèmes.
- **Un ver** I Il se propage sans hôte, souvent via les réseaux.
- **Un cheval de Troie (Trojan) I** Le cheval de Troie, à l'instar de sa version historique, se dissimule dans un programme apparemment légitime pour combattre de l'intérieur.
- **Un ransomware** I C'est un logiciel qui chiffre les fichiers et demande une rançon pour les déchiffrer (ex. : WannaCry, LockBit).
- **Un spyware** I Le Spyware espionne les activités de l'utilisateur (ex. : keylogger).
- **Un rootkit** I Un rootkit d issimule l'activité d'un malware sur un système.
- **Un adware** I Malware qui affiche de la publicité non sollicitée, parfois intrusive ou piégée.

LES MENACES INTERNES : VULNÉRABILITÉS HUMAINES ET DÉFAILLANCES ORGANISATIONNELLES

Si les attaques externes concentrent l'essentiel de l'attention médiatique, les menaces internes représentent pourtant une part significative des incidents de cybersécurité. Ces dernières sont d'autant plus redoutables qu'elles émanent de l'intérieur du système, souvent par des personnes disposant d'un accès légitime aux ressources critiques. Elles peuvent résulter d'actes intentionnels (sabotage, vol de données) ou d'erreurs involontaires (mauvaise manipulation, usage non autorisé de services).

Ces menaces soulignent l'importance d'une culture de la cybersécurité partagée et d'un encadrement rigoureux des pratiques numériques en interne. En matière de communication, elles imposent une gestion délicate : protéger la réputation de l'organisation sans stigmatiser les individus, rassurer les parties prenantes internes, tout en répondant aux exigences réglementaires.

Les principales menaces :

- **L'employé malveillant I** Acte volontaire de sabotage, vol ou divulgation de données.
- **L'erreur humaine** I Mauvaise manipulation, configuration incorrecte, négligence (mot de passe faible, lien mal cliqué...).
- **Le Shadow IT I** Utilisation non contrôlée de logiciels ou services cloud par les employés.

LES ATTAQUES SUR LES SYSTÈMES ET RÉSEAUX

Les attaques ciblant les systèmes et réseaux constituent le socle technique de nombreuses cybermenaces. Elles visent à perturber la disponibilité des services, à intercepter des communications ou à exploiter des vulnérabilités pour s'introduire dans les systèmes d'information. Leur diversité technique et leur potentiel de nuisance exigent une vigilance constante, tant au niveau de l'architecture des réseaux que des applications utilisées.

Ces attaques peuvent provoquer des interruptions de service, des pertes de données, ou ouvrir la voie à des compromissions plus profondes. Du point de vue de la communication, elles soulèvent des enjeux spécifiques : expliquer un incident technique de manière compréhensible, sans affoler inutilement ; informer les clients d'une indisponibilité tout en préservant l'image de fiabilité ; et répondre aux exigences de transparence des autorités compétentes.

Les principales attaques :

- **Le déni de service (DoS)** I Saturation d'un système pour le rendre indisponible.
- **Le déni de service distribué (DDoS)** : Même principe, mais depuis de multiples sources.
- **Le man-in-the-middle (MITM)** : Interception des communications entre deux parties.
- **Le sniffing** : Capture des données transitant sur un réseau (souvent avec un logiciel espion).
- **L'injection SQL** : Insertion de requêtes malveillantes dans une base de données via un champ de formulaire.
- **L'exploitation de failles (zero-day)** : Attaque basée sur une vulnérabilité encore inconnue du fournisseur.
- **Le cross-site scripting (XSS)** : Injection de scripts dans des pages web vues par d'autres utilisateurs.

LES MENACES LIÉES À LA CHAÎNE D'APPROVISIONNEMENT

La multiplication des services externalisés, des composants logiciels tiers et des solutions cloud a considérablement élargi la surface d'exposition des organisations. Désormais, une part significative des attaques informatiques ne cible plus directement l'entreprise elle-même, mais ses partenaires, sous-traitants ou fournisseurs — souvent considérés comme les maillons les plus vulnérables de l'écosystème numérique.

Les attaques sur la chaîne d'approvisionnement peuvent prendre plusieurs formes :

- **Des attaques indirectes via un prestataire,** comme ce fut le cas lors de la compromission de SolarWinds en 2020, où une mise à jour logicielle vérolée a permis l'intrusion dans de multiples organisations à l'échelle mondiale ;
- **Des compromissions logicielles,** consistant à insérer du code malveillant dans une bibliothèque, un module ou une mise à jour d'un produit tiers, afin de contourner les contrôles de sécurité habituels ;
- **Des vulnérabilités chez des fournisseurs de services** cloud, dont la compromission peut entraîner un accès élargi à des données sensibles ou à des environnements critiques partagés entre plusieurs clients.

Ces menaces, difficilement détectables, soulèvent des défis majeurs en matière de gouvernance, de contrôle des tiers, et de cybersécurité contractuelle. En matière de communication de crise, elles présentent une double difficulté : la dilution des responsabilités, d'un part, qui peut rendre floue la capacité de l'organisation à reconnaître sa part de responsabilité ou à justifier l'incident auprès de ses parties prenantes ; la gestion coordonnée de la parole, d'autre part. notamment lorsque plusieurs acteurs sont impliqués et que les délais de reconnaissance ou de notification diffèrent entre les partenaires.

Dans ce contexte, il est essentiel d'intégrer dans les plans de communication de crise des scenarii liés à la chaîne d'approvisionnement, en identifiant à l'avance es prestataires critiques, les engagements contractuels de transparence, et les procédures d'escalade ou de déclaration conjointe en cas de compromission.

LES CAMPAGNES D'INGÉRENCE ET DE DÉSINFORMATION

Au croisement des menaces cyber, informationnelles et géopolitiques, les campagnes d'ingérence et de désinformation représentent un vecteur d'attaque de plus en plus fréquent et structurant. Ces actions malveillantes visent moins les systèmes techniques que les perceptions, la réputation ou la cohésion interne d'une organisation. Elles exploitent les vulnérabilités cognitives et informationnelles des individus pour semer le doute, déstabiliser ou influencer.

Ces campagnes s'appuient sur des outils de plus en plus sophistiqués :

- **Les deepfakes,** qui permettent de produire des vidéos ou enregistrements audio falsifiés, visuellement convaincants, pouvant faire croire à des propos ou des actes fictifs de dirigeants ou d'experts ;
- **Les faux comptes sur les réseaux sociaux,** utilisés pour infiltrer des communautés en ligne, amplifier artificiellement certains discours, ou semer des divisions internes à l'organisation ;
- Les **fake news virale**s, souvent diffusées via des canaux grand public, qui associent mensonges, approximations et émotions fortes pour maximiser leur diffusion et créer un effet de sidération ou de défiance.

Ces attaques peuvent accompagner une crise cyber technique (ransomware, vol de données) pour en aggraver les effets, ou constituer une offensive autonome dans une logique de guerre informationnelle. Elles visent notamment à :

- affaiblir la légitimité de la parole officielle de l'organisation ;
- provoquer une perte de confiance chez les collaborateurs, les clients ou les citoyens ;
- contraindre l'organisation à réagir dans l'urgence sur un terrain qu'elle ne contrôle pas (réseaux sociaux, forums, médias étrangers).

Face à ce type de menace, la stratégie de communication ne peut se limiter à la diffusion d'un message défensif. Elle suppose une capacité de veille renforcée, une réactivité accrue, des contre-discours crédibles, et la mobilisation rapide de relais internes et externes (experts, journalistes, communauté d'utilisateurs…). Elle impose également de préparer des scenarii de réponse à la désinformation, intégrés aux plans de gestion de crise, avec des canaux validés et des porte-parole formés à la réponse en environnement hostile.

ETAPE 2

CONNAÎTRE EN AMONT

LES ACTEURS ET LEUR RÔLE DANS LA CRISE

En cas d'attaque cyber, la communication avec les parties prenantes doit être à la fois rapide, maîtrisée et transparente pour mieux protéger la réputation de l'organisation, de limiter la propagation de la crise et de conserver la confiance des parties prenantes. Une communication efficace ne s'improvisant pas, il est essentiel d'avoir préparé un plan de gestion de crise cyber en amont. En voici les principales étapes.

CONNAÎTRE ET CARTOGRAPHIER L'ENSEMBLE DE SES PARTIES PRENANTES

La première étape de toute stratégie de communication de crise cyber consiste à identifier, qualifier et cartographier l'ensemble des parties prenantes susceptibles d'être impactées ou impliquées lors d'un incident. Cette cartographie constitue un prérequis essentiel, car elle permet de définir précisément qui doit être informé, dans quel ordre et avec quels messages.

Cette démarche s'apparente à l'élaboration d'un plan d'évacuation en cas d'incendie : elle repose sur une connaissance fine de l'environnement de l'organisation et **doit être actualisée régulièrement (au minimum une fois par an) pour refléter l'évolution des structures internes, des partenariats, des obligations réglementaires et des canaux de communication.** La cartographie distingue classiquement les parties prenantes internes et externes.

Concernant les parties prenantes internes

Elles doivent être informées très rapidement pour enclencher la réponse opérationnelle et assurer l'alignement stratégique de l'organisation. On y trouve notamment :

- La direction générale (COMEX), pour piloter les arbitrages de communication ;
- La DSI et le RSSI, acteurs centraux de la gestion technique de l'incident ;
- Des services ou groupes de travail spécifiques,
- Tous les collaborateurs qui doivent recevoir une information claire sur la situation, les consignes de sécurité à respecter et la posture de communication attendue (ex. : silence média, redirection vers un porte-parole désigné).

Concernant les parties prenantes externes

Selon la nature, la gravité et l'impact de l'attaque, un cercle plus ou moins large d'acteurs externes peut être concerné :

- **Les clients**, qui doivent être informés en cas de compromission de données ou d'interruption de service ;
- **Les partenaires et fournisseurs**, notamment s'ils partagent des systèmes d'information ou des flux de données avec l'organisation touchée ;
- **Les actionnaires**, pour préserver la transparence financière et anticiper les impacts réputationnels ou boursiers ;
- **Les autorités compétentes** (ANSSI, CNIL, procureur de la République, autorités sectorielles…), dont la notification est souvent obligatoire dans des délais contraints ;
- **Les médias**, qui peuvent relayer l'information de manière incontrôlée en l'absence de communication proactive ;
- **Le grand public,** en cas de forte médiatisation ou d'impact sociétal significatif.

Cette cartographie doit être intégrée dans le plan de gestion de crise cyber de l'organisation, assortie des coordonnées précises, des interlocuteurs clés, des canaux de communication privilégiés et des délais maximum d'alerte. Elle doit également anticiper les contraintes réglementaires spécifiques (RGPD, directives sectorielles, obligations liées aux OIV/FSN) et inclure des scénarios d'activation selon la typologie de l'incident.

N'hésitez pas dans sa V1 à faire une cartographie très exhaustive. Dans un premier temps, contentez-vous d'un simple listing Word que vous pouvez travailler en atelier avec vos équipes. Actualiser cette cartographie chaque année avec vos équipes permet de poursuivre la sensibilisation au sujet.

DEFINIR CLAIREMENT LA COMPOSITION DE SA CELLULE DE CRISE AVANT LA CRISE

C'est un fait : une communication maîtrisée lors d'une cyberattaque nécessite une gouvernance de crise préalablement structurée. Il est impératif que la cellule de communication s'inscrive pleinement dans la cellule de crise globale de l'organisation, sans en constituer un silo isolé. Toute absence de coordination peut entraîner une désorganisation majeure, se traduisant par une cacophonie interne, des messages contradictoires et une perte de contrôle sur la narration publique de l'événement. La constitution de cette cellule doit donc être anticipée pour ne pas être laissée à l'improvisation le jour de la crise.

Elle ne doit pas être réduite aux seuls communicants mais doit intégrer l'ensemble des expertises clés permettant de construire une parole cohérente, juridiquement conforme, techniquement exacte, et politiquement soutenable.

On y retrouve généralement :

- **Un responsable de l'activation**, garant du déclenchement formel de la cellule, habilité à en ordonner la mobilisation selon des critères prédéfinis (niveau de criticité, typologie d'impact, alerte ANSSI ou CNIL, etc.) ;
- **Un porte-parole désigné**, unique voix publique de l'organisation, capable d'incarner la position institutionnelle, de gérer la relation avec les médias et de porter les messages de transparence ou de résilience ;
- **Un référent technique,** souvent issu de la DSI ou du RSSI, chargé de traduire les éléments d'analyse informatique en messages compréhensibles pour des non-experts, et d'évaluer l'évolution de l'incident ;
- **Un référent juridique**, garant de la conformité des messages, notamment au regard du RGPD, des obligations de notification à la CNIL ou à l'ANSSI, ou des éventuelles procédures contentieuses ou pénales à venir ;
- **Un représentant de la direction générale**, dont la présence permet de sécuriser les arbitrages sensibles (reconnaissance publique d'un incident, communication proactive sur une compromission de données, décision d'indemnisation, etc.).

Chaque membre de la cellule doit être identifié nominativement, avec ses coordonnées directes, ses plages de disponibilité, et ses prérogatives. Ces données doivent figurer dans une matrice de crise tenue à jour, accessible rapidement, et testée régulièrement dans le cadre d'exercices de simulation.

Il est par ailleurs recommandé d'organiser des points de revue annuels pour valider la composition de la cellule et tester la réactivité des membres, notamment en cas de changements de poste, de mobilité interne ou de départs. Ce travail de structuration est une condition sine qua non d'une communication de crise rapide, alignée et crédible.

FONCTION	NOM	TITRE	PRÉROGATIVES	CONTACT
Responsable de l'activation	[Nom]	[Fonction]	Déclenche la cellule, valide les seuils d'alerte	[Coordonnées]
Porte-parole désigné	[Nom]	[Fonction]	Porte les messages officiels à l'externe	[Coordonnées]
Référent technique	[Nom]	[Fonction]	Fournit l'analyse technique et son évolution	[Coordonnées]
Référent juridique	[Nom]	[Fonction]	Garantit la conformité des messages	[Coordonnées]

POSER SES PROCESS DE VALIDATION

En situation de crise cyber, chaque message diffusé – qu'il soit interne, externe, ou à destination des autorités – doit faire l'objet d'un circuit de validation préétabli pour éviter les maladresses, les contradictions ou les pertes de temps critiques. Il est essentiel de déterminer en amont qui valide quoi, en fonction du type de communication (technique, RH, institutionnelle, presse, etc.).

Pour cela, la cellule de crise doit se doter d'un référentiel clair des circuits de validation, incluant les niveaux d'information, de consultation ou d'approbation pour chaque typologie de message. Ce dispositif doit concilier rapidité, traçabilité et sécurité, et pouvoir être activé même en cas d'indisponibilité temporaire de certains acteurs. Il s'appuie sur des outils simples (tableaux, schémas de validation, grilles d'astreinte) à maintenir à jour, testés régulièrement lors d'exercices.

L'objectif visé par le référentiel à créer :

- définir clairement les rôles. La typologie doit distinguer avec justesse les différentes responsabilités, en évitant les confusions fréquentes entre auteur, validant et diffuseur. La présence d'un rôle « Informé » est judicieuse pour éviter la surcharge des circuits de validation.
- Hiérarchiser efficacement le processus de validation. La dissociation entre expertise (consulté), décision (validant) et exécution (diffuseur) permet de fluidifier la prise de décision, surtout sous contrainte de temps.
- Donner des exemples concrets. L'application à un cas spécifique (message interne aux collaborateurs en cas de ransomware) permet de visualiser immédiatement l'intérêt opérationnel de la matrice.
- Anticiper d'éventuelles absences

EXEMPLE : MESSAGE INTERNE AUX COLLABORATEURS - CONSIGNES EN CAS DE RANSOMWARE

FONCTION	RÔLE	COMMENTAIRE / RESPONSABILITÉ	BACK UP DESIGNE
RSSI	Responsable	Rédige le message avec l'expertise technique	Adjoint RSSI / Responsable CERT interne
Direction des ressources humaines (DRH)	Consulté	Apporte un éclairage RH (congés, horaires, tension sociale…)	DRH adjoint(e) ou RRH
Direction des ressources humaines (DRH)	Consulté	Vérifie conformité RGPD, obligations légales	Juriste cybersécurité
Direction de la communication	Validant	Valide le message final, engage la parole de l'organisation	Directeur adjoint de la communication
Responsable de la communication	Diffuseur	Transmet le message via les canaux internes définis	Chargé de communication
Direction générale (DG)	Informé	Est tenue informée pour suivi stratégique	Chef de cabinet / Secrétaire général
Autres directions (non impliquées)	concerné	Ne participent pas à ce message	-

ETAPE 3

IDENTIFIER EN AMONT

SES OBJECTIFS DE COMMUNICATION PAR TYPOLOGIE DE CIBLE

IDENTIFIER SES OBJECTIFS DE COMMUNICATION EN FONCTION DES DIFFÉRENTES PARTIES PRENANTES

En vous appuyant sur votre cartographie, vous pouvez facilement clarifier vos objectifs de communication. Un exemple très générique ci-dessous.

Exemples d'objectifs de communication vers les parties prenantes internes

Le COMEX (Comité exécutif)

- Informer rapidement et clairement de la nature, de l'ampleur et des conséquences potentielles de l'attaque.
- Présenter les premières mesures prises (techniques, juridiques, communication) et les étapes du plan de gestion de crise.
- Aider à la prise de décision stratégique en fournissant des éléments fiables et synthétiques.
- Préparer les membres à s'exprimer de manière cohérente en externe si nécessaire.

DSI / RSSI

- Assurer une coordination fluide avec la cellule de crise et les prestataires techniques.
- Clarifier les priorités opérationnelles (confinement, remédiation, reprise d'activité).
- Valoriser leur rôle dans la réponse à la crise tout en évitant les reproches immédiats.
- Favoriser la circulation d'informations techniques fiables pour éviter les interprétations erronées.

Tous les collaborateurs

- Informer de manière transparente et didactique, sans créer de panique.
- Expliquer les consignes concrètes (ne pas utiliser certains outils, changement de mots de passe, vigilance accrue).
- Maintenir un climat de confiance et d'engagement, en insistant sur le rôle actif de chacun dans la réponse.
- Prévenir la diffusion de rumeurs internes ou de communications externes incontrôlées.

Exemples d'objectifs de communication vers les parties prenantes externes

Les clients

- Reconnaître l'incident de manière factuelle, sans minimisation ni dramatisation.
- Rassurer sur la protection de leurs données (ou expliquer les risques s'il y a eu fuite).
- Expliquer les mesures prises pour sécuriser les systèmes et prévenir de futures attaques.
- Préserver la relation de confiance et limiter les départs ou réclamations.

Les partenaires et fournisseurs

- Informer des impacts éventuels sur les systèmes interconnectés ou les processus communs.
- Rechercher la coopération pour contenir ou analyser l'attaque si leurs systèmes sont potentiellement affectés.
- Préserver la confiance contractuelle, éviter les litiges.
- Renforcer à moyen terme les clauses de cybersécurité dans les contrats et pratiques de la chaîne d'approvisionnement.

Les actionnaires et investisseurs

- Fournir une information transparente, dans le respect du droit boursier le cas échéant.
- Rassurer sur la capacité de l'organisation à gérer la crise et à préserver sa valeur à long terme.
- Montrer la mobilisation du management et des experts pour limiter les impacts opérationnels et réputationnels.
- Préparer d'éventuelles questions lors d'assemblées générales ou points financiers.

Les régulateurs (ANSSI, CNIL, etc.)

- Notifier rapidement l'incident dans les délais réglementaires.
- Fournir des informations claires, structurées, et coopérer pleinement dans l'analyse et la remédiation.
- Montrer la conformité de l'organisation à ses obligations légales (RGPD, directive NIS2, etc.).
- Prévenir les sanctions en adoptant une posture proactive et transparente.

Les médias

- Contrôler la narration publique de l'incident pour éviter les spéculations dommageables.
- Fournir un message centralisé, clair, et cohérent avec la communication vers les autres parties prenantes.
- Limiter l'impact réputationnel et montrer que l'organisation agit avec sérieux, rapidité et responsabilité.
- S'exprimer dans un ton mesuré, factuel, sans verser dans la langue de bois.

Le grand public

- Informer avec pédagogie, surtout si l'incident a un impact sur des services d'intérêt général.
- Démontrer la transparence et la responsabilité sociale de l'organisation.
- Préserver la réputation de la marque, surtout dans les secteurs sensibles (santé, énergie, transport).
- Répondre aux inquiétudes collectives et prévenir une amplification de la crise via les réseaux sociaux.

Voici un exemple de tableau qui peut vous permettre d'analyser très vite la situation à laquelle vous êtes confrontez avec des exemples d'objectifs type. Lors de la crise, vous n'avez plus qu'à cocher les objectifs de communication qui vous concernent.

Type d'attaque	Partie prenante impactée	Partie prenante à informer	Objectif de communication (message à faire passer)
[Nom de l'attaque]	INTERNE	COMEX	Informer rapidement des faits et impacts,
			Permettre une décision stratégique éclairée.
		DSI / RSSI	Coordonner l'action technique et la communication avec les autres cellules.
		Tous les collaborateurs	Expliquer les consignes
			Rassurer
			Eviter les rumeurs et mobiliser les équipes donner les éléments de langage interne
	EXTERNE	Clients	Préserver la confiance, indiquer les impacts éventuels et les mesures prises.
		Partenaires / fournisseurs	Clarifier les effets éventuels sur les flux ou systèmes interconnectés.
		Actionnaires / investisseurs	Rassurer sur la gouvernance, la maîtrise de la crise et les conséquences financières.
		Régulateurs (ANSSI, CNIL, etc.)	Respecter les obligations légales,
			Collaborer activement à la remédiation
		Médias	Contrôler le récit public,
			Montrer transparence et responsabilité.
		Grand public	Informer sans alarmer,
			Démontrer la posture éthique et la maîtrise.

ETAPE 4

DEFINIR LES BONS CANAUX ET PRÉPARER LES BONS MESSAGES

En situation de crise cyber, la pertinence du message ne suffit pas : encore faut-il qu'il parvienne, au bon moment, à la bonne audience, par le canal le plus adapté. Le choix du canal et la formulation du message ne sont jamais neutres ; ils conditionnent directement la compréhension, l'adhésion et la réaction des parties prenantes. Une communication trop technique adressée à des clients grand public, ou une information trop générique transmise à une autorité réglementaire, peut nuire à la clarté, engendrer des malentendus, ou alimenter la défiance.

Il convient donc de calibrer avec précision chaque message selon sa cible, son niveau d'expertise, sa sensibilité au risque et son degré d'exposition à l'incident. Cette exigence suppose une double réflexion : sur le fond (contenu, ton, degré de transparence, reconnaissance éventuelle d'une faille) et sur la forme (canal utilisé, timing, fréquence, identité de l'émetteur). Courriel interne, communiqué de presse, espace dédié sur le site web, contact personnalisé pour les clients à haut enjeu, point presse ou publication sur les réseaux sociaux : chaque canal a ses usages, ses forces et ses limites.

Cette étape, qui doit être anticipée dès la phase de préparation, repose sur des scénarii préétablis, testés, et adaptés aux spécificités de l'organisation. Elle constitue un levier majeur pour limiter la propagation de la crise, maintenir la confiance, et maîtriser la narration publique de l'événement.

LES DIFFÉRENTS CANAUX DE COMMUNICATION

Les canaux de communication internes

- **Le téléphone** / les appels directs. Rapide, personnalisé, utile pour les décisions urgentes ou les échanges confidentiels (COMEX, DSI, juridique).
- **Les SMS ou notifications mobiles sécurisées.** Pour alerter immédiatement un groupe restreint en dehors des heures de bureau ou en situation de mobilité.
- **La messagerie instantanée professionnelle (Slack, Teams, Mattermost, Rocket.Chat…).** Communication rapide, structurée en canaux dédiés (ex. : #crise-cyber), utile pour la coordination de la cellule de crise.
- **Email interne (messagerie professionnelle)** Canal formel pour transmettre des consignes, faire des rappels ou adresser des messages à large échelle.
- **L'intranet ou le portail RH** I Pour diffuser des informations générales ou documenter la situation dans le temps (FAQ, état de l'incident, procédures à suivre).
- **Les réunions physiques ou visioconférences (Zoom, Webex, Teams…)** Pour organiser des points de situation, arbitrer collectivement ou mobiliser un groupe-clé (cellule de crise, management intermédiaire, etc.).
- **L'affichage physique dans les locaux** I En cas de coupure SI ou pour relayer rapidement une consigne essentielle (poste de sécurité, salle de pause, hall d'entrée).

Les canaux de communication externes

- **L'Email externe personnalisé (clients, fournisseurs, partenaires)** I Le canal privilégié pour informer directement des parties tierces affectées, avec un contenu adapté à leur situation (ex. : fuite de données, interruption de service).
- **Le communiqué de presse** I Format formel pour adresser un message institutionnel aux médias et au public ; utile en cas de médiatisation ou d'incident majeur.
- **La conférence ou point presse** I Permet d'incarner la parole officielle, de répondre aux questions, de rassurer ou de rétablir la vérité.
- **Le site web de l'organisation (page d'accueil, pop-up, espace de crise dédié)** I Pour centraliser les informations officielles, publier des mises à jour et relayer les consignes pratiques.

Concrètement, le plus efficace est de rajouter une colonne dans le tableau précèdent

Type d'attaque	Partie prenante impactée	Partie prenante à informer	Objectif de communication (message à faire passer)	Canaux d'information privilégiés
[Nom de l'attaque]	INTERNE	COMEX	Informer rapidement des faits et impacts,	Téléphone / SMS / doublé d'un récapitulatif écrit très précis.
			Permettre une décision stratégique éclairée.	Téléphone / SMS / réunion express (Visio/présentielle)
		DSI / RSSI	Coordonner l'action technique et la communication avec les autres cellules.	Réunion (Visio/présentielle)
		Tous les collaborateurs	Expliquer les consignes	Réunion de service / rappel par mail depuis de mail de la direction / ou du DSI / Affichage
			Rassurer	Réunion de service / Mail / Affichage
			Eviter les rumeurs et mobiliser les équipes donner les éléments de langage interne	Réunion de service / Mail / Affichage

RÉDIGER EN AMONT SES MESSAGES TYPE ET ÉLÉMENTS DE LANGAGE

Il est important ensuite de préparer des éléments de langage ou messages type (déjà pré-validés lors de la constitution de votre malette de crise) pour n'avoir plus qu'à les ajuster lorsque la crise arrivera. Pensez bien aux éléments dont vos cibles de communication ont besoin.

Exemple :
Informer le COMEX sur un ransomware.
De quoi votre COMEX a besoin ?

- de comprendre de quelle menace il s'agit
- de comprendre les impacts sur l'organisation
- de savoir ce qu'il y a à décider rapidement
- de savoir qui fait quoi et de suivre en temps réel l'évolution.

Ci après un exemple message à diffuser lors d'une réunion sécurisée :

Madame, Monsieur,
Nous vous informons qu'un incident de cybersécurité de type ransomware est en cours de traitement au sein de nos systèmes d'information. La cellule de crise a été activée à [heure], conformément au protocole établi.

1. Nature de la menace
Un ransomware (logiciel de chiffrement malveillant) a été détecté sur [nombre] serveurs/terminaux, à [heure précise].
Le malware identifié est [nom du ransomware si connu – ex. LockBit, BlackCat, ou "inconnu à ce stade"].
Le mode opératoire semble indiquer [préciser si attaque automatisée, ciblée, intrusion préalable, etc.].
La demande de rançon est actuellement de [montant, en cryptomonnaie ou autre], avec une échéance fixée à [date/heure].

2. État de la situation (à [heure])
- Systèmes affectés : [serveurs, applicatifs, messagerie, outils métiers, etc.]
- Fonctions critiques impactées : [préciser si facturation, production, logistique, etc.]
- Données chiffrées ou inaccessibles : [oui/non – préciser l'étendue]
- Propagation : en cours / circonscrite / inconnue
- Sauvegardes disponibles : [oui/non – validées ou en cours de vérification]
- Intrusion externe identifiée ? : [oui/non/suspectée]

3. Actions engagées
- Isolation des systèmes concernés : réalisée à [heure]
- Activation de la cellule de crise : [heure]
- Expertise technique externe mobilisée : [nom du prestataire / ANSSI si applicable]
- Notification à l'ANSSI / CNIL : prévue / effectuée / non requise à ce stade
- Communication interne : consignes transmises à l'ensemble des collaborateurs (cf. canal)
- Analyse des sauvegardes / plan de reprise : en cours

4. **Prochaines étapes**
- Évaluation complète de l'étendue de l'attaque sous 3 heures
- Préparation d'un message externe (clients / partenaires), à valider avec vous
- Arbitrage à venir sur réponse à la demande de rançon (préparation de scenarii avec le juridique)
- Points réguliers toutes les [2/4] heures

5. Vos éléments de décision à ce stade
- Valider la stratégie de communication externe (proactive ou différée)
- Décider du niveau d'information des actionnaires et du conseil d'administration
- Autoriser (ou non) la mobilisation de moyens exceptionnels (expertise tierce, prestataire technique, contact avec autorités judiciaires)

Nous vous tiendrons informés en temps réel. **Pour l'instant, nous suivons le process de crise classique** (Nom / numéro) / éventuellement le lien.

Prochain point d'étape prévu à [heure].

Bien cordialement,
[Nom du RSSI / Directeur de la communication / Coordinateur crise cyber]
Cellule de crise cybersécurité
[Coordonnées de contact en cas d'urgence directe]

Exemple de message à l'attention des collaborateurs (Objectif : éviter la panique, les rumeurs)

Objet : Incident de sécurité informatique en cours – consignes immédiates

Chers collègues,
Nous faisons actuellement face à un incident de sécurité de type ransomware, détecté ce [jour] à [heure].
Ce type d'attaque vise à chiffrer des fichiers ou des systèmes afin d'en bloquer l'accès.
La cellule de crise a été immédiatement activée. Une équipe dédiée traite la situation en lien avec nos experts internes et, le cas échéant, des partenaires spécialisés.

Ce que nous savons à ce stade :

- L'attaque a été détectée sur [zone impactée – ex. : certains serveurs internes / postes utilisateurs / applications métier].
- Des investigations sont en cours pour évaluer précisément l'étendue et l'origine de l'attaque.
- À ce stade, [les données de production ne sont pas affectées / une partie du SI est inaccessible / l'incident est contenu – à adapter selon le cas].

Consignes immédiates :
Merci d'appliquer ces mesures sans délai :

1. Ne pas redémarrer votre ordinateur si vous constatez un comportement anormal (fenêtre de rançon, lenteur, message suspect).
2. Déconnecter immédiatement votre poste du réseau (câble Ethernet ou Wi-Fi).
3. Ne pas cliquer sur aucun lien ou pièce jointe suspecte, y compris dans les messages internes.
4. Signaler toute activité inhabituelle à l'adresse suivante : [adresse email ou numéro de la cellule de crise].
5. Respecter strictement les canaux officiels de communication. Toute diffusion d'information non validée (internes, médias, réseaux sociaux) est interdite.

Ce que nous faisons :
Nos équipes techniques sont mobilisées pour :

- contenir l'incident,
- évaluer les impacts,
- rétablir les services dans les meilleures conditions de sécurité.

Nous vous tiendrons informés régulièrement de l'évolution de la situation via [canal utilisé : email, intranet, Slack, etc.].

Rappel : vous êtes un maillon essentiel de la sécurité collective.
En appliquant rigoureusement ces consignes, vous contribuez à limiter les conséquences de cette attaque.
Nous comptons sur votre vigilance et votre professionnalisme.

Merci de votre attention,
[Nom, fonction]
Au nom de la cellule de crise cybersécurité
[Coordonnées ou canal de contact]

Exemple de message type à l'attention à destination des clients ou partenaires externes. l'objectif : respecter les principes de transparence mesurée, de responsabilité assumée, et de maîtrise du ton.

Objet : Information importante – incident de sécurité en cours

Madame, Monsieur,
Nous souhaitons vous informer qu'un incident de sécurité informatique affecte actuellement une partie de nos systèmes. Il s'agit d'une attaque par ransomware, détectée ce [jour] à [heure], dont le traitement est en cours.

Ce que nous savons à ce stade :

- L'attaque a entraîné le chiffrement de certains fichiers ou services.
- Nos équipes techniques, en lien avec des experts externes, ont activé les mesures de confinement nécessaires.
- À ce stade, aucune compromission de vos données n'a été identifiée, mais des analyses approfondies sont en cours pour confirmer ce point.

Mesures en cours :

- Isolation des systèmes affectés
- Investigation technique pour déterminer l'origine et l'étendue de l'incident
- Mobilisation de notre cellule de crise, incluant des spécialistes en cybersécurité et en conformité réglementaire
- Préparation d'un plan de reprise et de communication progressive selon l'évolution de la situation

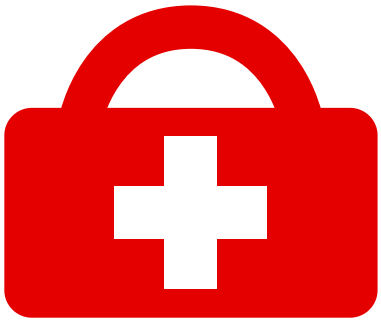
Ce que nous nous engageons à faire :

- Vous tenir informé(e) de manière transparente de toute évolution significative
- Vous alerter immédiatement en cas de confirmation d'impact sur vos données ou vos services
- Mettre en œuvre tous les moyens nécessaires pour restaurer un fonctionnement sécurisé dans les meilleurs délais

Nous comprenons les inquiétudes que ce type de situation peut susciter et mettons tout en œuvre pour la gérer avec rigueur, responsabilité et efficacité.
Pour toute question ou besoin spécifique, vous pouvez contacter notre cellule dédiée à l'adresse suivante :
[adresse email dédiée]
[numéro de téléphone du support exceptionnel, si applicable]

Nous vous remercions pour votre confiance et votre compréhension.
Bien cordialement,

[Nom + fonction du signataire (ex. : Directeur général / Responsable des relations clients)]
Au nom de l'équipe de gestion de crise cybersécurité
[Nom de l'organisation]



NOS DERNIÈRES RECOMMANDATIONS :
Rédigez vos messages en amont ET FAITES LES VALIDER pour vous constituer une malette de crise opérationnelle.
N'hésitez pas également à archiver les messages que vous recevez d'autres structures.

[redacted]

State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

July 8, 2022

RE: **Notice of Data Breach**

Dear [redacted]

This letter is to inform you of a recent security incident that involved an unauthorized release of your personal information by the California Department of Justice (DOJ). This information primarily relates to individuals who were denied or granted a concealed and carry weapons (CCW) permit between 2011-2021, and was disclosed in connection with an update to our Firearms Dashboard Portal. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect your identity, should you feel it is appropriate to do so.

What Happened
As announced on June 29, 2022, personal information was disclosed on June 27, 2022 in connection with the update of DOJ's Firearms Dashboard Portal. After DOJ learned of the data exposure, the Department took steps to remove the information from public view and shut down the Firearms Dashboard. The dashboard and data were available for less than 24 hours.

What Information Was Involved
As of the date of this letter, the information that we have determined was exposed includes full name, date of birth, address, gender, race, CCW license number, California Information Index number (which is automatically generated during a fingerprint check for a CCW or for another purpose), and other government-issued identifiers. In some cases, exposed information may also include driver's license number, and internal codes corresponding to the statutory reason that a person is prohibited from possessing a firearm. Social Security numbers or any financial information were **not** disclosed as a result of this event.

What We Are Doing
We are working to improve security, mitigate risk, and have launched an investigation into how this occurred at DOJ. We have removed the information from public view, shut down the Firearms Dashboard, and are contacting individuals who have been impacted by the breach to provide additional information and resources for them. Additionally, we are conducting a review of our policies and procedures and working to implement additional security measures to protect the security of information in our possession and communicating regularly with our law enforcement partners throughout the state.

As an added precaution and to provide direct assistance to those impacted, we have established a call center to address any questions you may have. We are also offering complimentary access to credit monitoring services through IDX, which includes: 12 months of triple-bureau credit monitoring, CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

1300 I STREET • SUITE 1740 • SACRAMENTO, CALIFORNIA 95814

VOTRE OBJECTIF

AGIR VITE

SANS PRÉCIPITATION

DÈS LA DÉTECTION DE L'INCIDENT

La phase initiale d'une cyberattaque est déterminante. Dès la détection d'un incident, il est impératif d'activer les premières mesures sans attendre, tout en évitant toute précipitation susceptible d'aggraver la situation ou de compromettre les preuves.

Agir vite ne signifie pas agir dans l'urgence émotionnelle, mais selon un protocole prédéfini, testé, et maîtrisé. C'est cette discipline opérationnelle qui permet à la fois de contenir techniquement l'attaque, de préserver les éléments de preuve pour l'analyse forensique, et de poser les bases d'une communication structurée, cohérente et crédible.