CHECKLIST AVANT UNE CRISE CYBER

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

CHECKLIST PENDANT UNE CRISE CYBER

- ○ Mettre en place une organisation spécifique de crise de votre équipe communication avec une répartition des rôles (coordination, perception et réaction) et des missions.
- ○ Réaliser un état des lieux des faits, de la situation en matière de communication et du contexte.
- ○ Proposer à vos dirigeants une posture de communication à adopter : proactive ou réactive.
- ○ Définir vos objectifs de communication principaux (expliquer, informer, rassurer, préserver l'image et la réputation de l'entité et faire changer les comportements).
- ○ En cas de communication réactive, questionner le moment et la pertinence d'une première communication.
- ○ En cas de communication proactive, communiquer rapidement uniquement des informations vérifiées, ne pas s'engager sur une date de retour à la normale précise, informer régulièrement et occuper l'espace médiatique si cela est possible.

CHECKLIST PENDANT UNE CRISE CYBER

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

CHECKLIST APRÈS UNE CRISE CYBER

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