L'ART DE SURVIVRE AUX CRISES

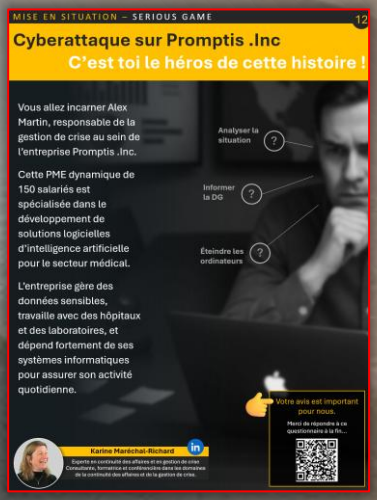
CRISE & RÉSILIENCE

Pays de nos auteurs : France, Canada, Luxembourg, Belgique, Nouvelle-Zélande, Roumanie, Suisse

NUMÉRO 11 – Juillet 2025

MAGAZINE

ORGANISATIONNELLE – INFORMATIQUE – SÉCURITÉ CIVILE – FINANCIÈRE – APPROVISIONNEMENT – ETC.



NOUVEAU SERIOUS GAME

Cyberattaque sur Promptis Inc.

C'est toi le héros de cette histoire !

DOSSIERS DU MOIS

Cadre de gestion de crise, lutte contre le terrorisme.

Magazine Crise & Résilience

La résilience, un article à la fois

Nombre d'auteurs

+ de 70

Experts de leurs domaines

Nombre d'articles et dossiers

+ de 130

Des centaines de pages de contenu utile

Nombre d'impression totale
(sur LinkedIn)

+ de 150k

ABONNEZ-VOUS GRATUITEMENT

Le monde traverse une période de grande incertitude et de changement et il est plus important que jamais de se préparer à affronter ces défis. Devenez résilient !

www.criseetresilience-magazine.com

Édito

Blackout, cyberattaque, crise terroriste, rupture d'approvisionnement… Le monde ne nous laisse aucun répit.

Mais dans la tempête, une conviction s'impose : la résilience n'est plus une option, c'est la clé pour transformer chaque crise en moteur de progrès.

Dans ce numéro, **Alexandre Fournier** parle du blackout historique espagnol : un électrochoc qui révèle la vulnérabilité de nos infrastructures et l'urgence d'innover.

Frédéric Cuvelier, lui, bouleverse nos certitudes : et si l'adaptation et le lâcher-prise étaient les véritables super-pouvoirs du leader en temps de crise ?

Lina Kolesnikova dévoile comment un cadre de gestion de crise devient une arme stratégique face au terrorisme.

Pierre Aubry et **Magali Marti** vous surprendront avec un allié inattendu : le cheval, partenaire unique pour renforcer leadership, confiance et cohésion d'équipe.

Raphaël de Vittoris rappelle que la gestion de crise s'apprend, et que la pédagogie est notre meilleur atout pour progresser.

René-Sylvain Bédard, quant à lui, renverse les idées reçues : la cybersécurité peut devenir un véritable moteur de croissance, bien au-delà de la simple protection.

Tanguy Bornet défend l'anticipation comme art stratégique.

Timothy Mirthil de Segonzac nous partage le média training et ce que cela apporte dans une communication de crise.

Virginie Janty vous fait découvrir une ressource insoupçonnée pour gérer le stress : votre alimentation.

Exclusif : Passez à l'action ! Testez vos réflexes avec "Cyberattaque sur Promptis Inc.", notre **SERIOUS GAME Réalisé par Karine Maréchal-Richard**. Vous êtes le héros, vous prenez les décisions, vous vivez les conséquences. Saurez-vous éviter le désastre ?

Avec ces perspectives inédites, nous vous offrons bien plus qu'une lecture : une boîte à outils pour affronter l'incertitude avec confiance et créativité.

Que vous soyez dirigeant, expert ou simplement curieux, Crise & Résilience Magazine reste votre boussole pour naviguer dans les turbulences.

Bonne lecture, et surtout… bonne résilience !

L'équipe éditoriale

Sommaire

NOTE : Les articles sont classés par ordre alphabétique des prénoms

Partagez votre expertise dans notre magazine !

Vous êtes expert en résilience et gestion de crise ? Rejoignez-nous pour inspirer nos lecteurs avec des articles innovantes sur des sujets en lien avec la résilience des entreprises et de la société en générale.

Envoyez votre résumé d'article à **info@crise-resilience.com** et partagez vos retours d'expérience et conseils pratiques pour renforcer la résilience des organisations.

Contribuez dès maintenant à développer une culture de résilience !

Direction de la publication : A.Fournier - **Création graphique :** Alfo65 - **Crédit photo :** FreePix – Dall-E 3 – MidJourney – **Édition : Crise&Résilience** - Québec (Qc), Canada – **Nous contacter :** info@crise-resilience.com

Blackout historique en Espagne : causes, impacts et leçons à tirer

Le lundi 28 avril 2025, l'Espagne et le Portugal ont été frappés par un blackout électrique d'une ampleur inédite, plongeant des dizaines de millions de personnes dans le noir pendant plusieurs heures.

Alexandre Fournier

Expert en gestion et simulation de crise

Consultant, formateur et conférencier dans les domaines de la continuité des affaires et de la gestion de crise depuis 30 ans.

Cet événement, parmi les plus graves qu'ait connu l'Europe en matière d'énergie, a mis en lumière la vulnérabilité des infrastructures critiques et la dépendance de nos sociétés à l'électricité.

Retour sur les faits, les impacts majeurs et les enseignements à retenir.

Chronologie de la panne

La panne a débuté à 12h33, heure espagnole, affectant simultanément l'ensemble de la péninsule ibérique et une partie du sud-ouest de la France.

En quelques secondes, la demande électrique a chuté de moitié, passant de 27 500 MW à 15 000 MW, entraînant l'arrêt automatique de plusieurs centrales, y compris des centrales nucléaires espagnoles, conformément aux procédures de sécurité.

Le rétablissement du courant a commencé dans la soirée, et plus de 92 % du territoire espagnol était réalimenté en électricité dès le lendemain matin.

Au Portugal, 2,5 millions de foyers sur 6,5 millions avaient retrouvé l'électricité dès la nuit suivante.

La situation s'est normalisée en moins de 24 heures, mais les conséquences se sont fait sentir bien au-delà de la simple coupure de courant.

Impacts majeurs sur la population

👉Mise en danger directe de vies humaines

Le bilan humain est lourd : au moins **sept décès** directement liés à la panne ont été recensés, principalement parmi des personnes âgées ou dépendantes de dispositifs médicaux à domicile.

Une intoxication au monoxyde de carbone, due à l'utilisation d'un générateur pour alimenter une machine à oxygène, et un incendie déclenché par une bougie ont été signalés.

Ces drames soulignent la vulnérabilité des personnes fragiles lors de telles crises.

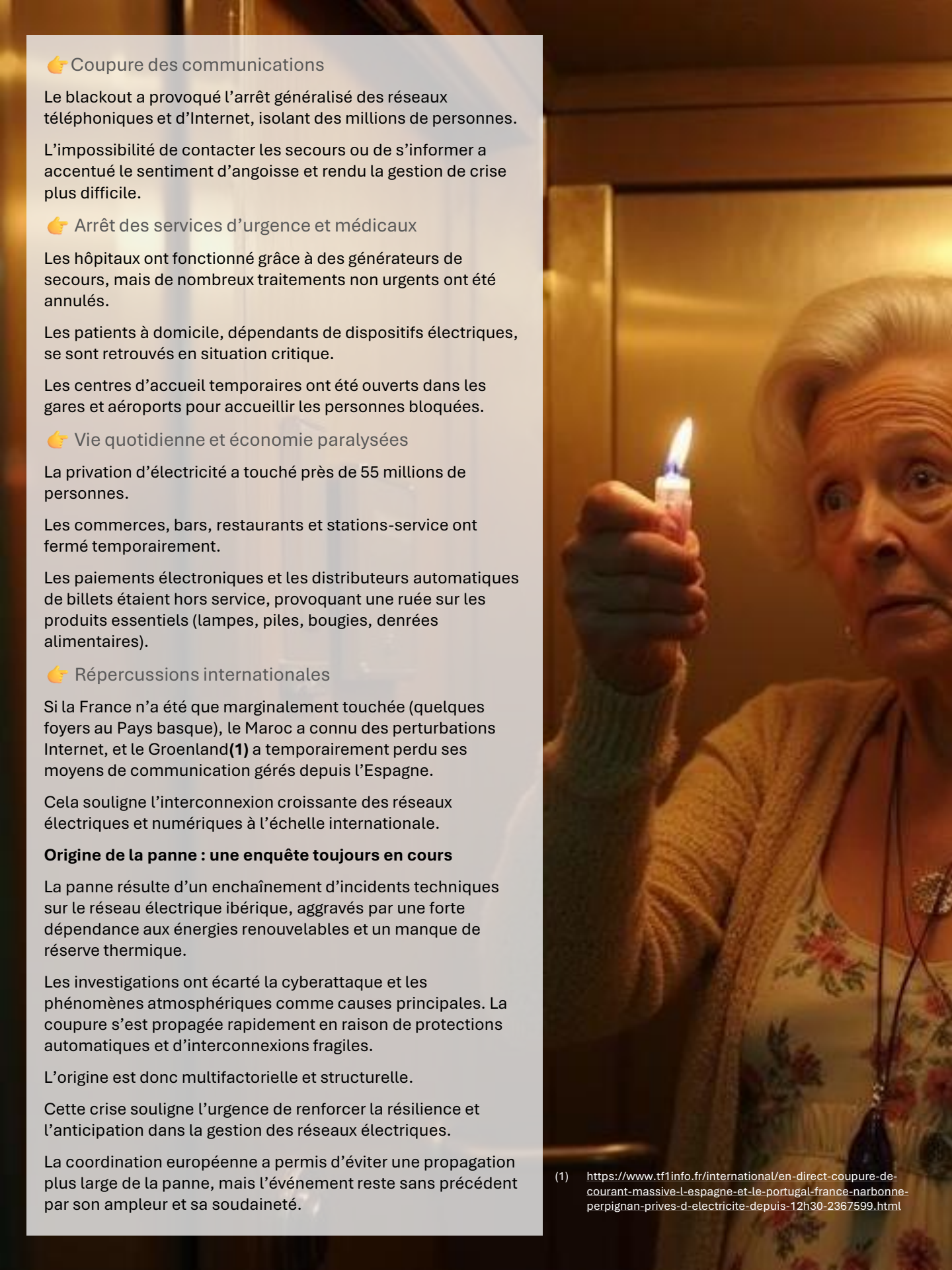
👉Blocage massif dans les transports

Plus de 35 000 passagers ont été bloqués dans 116 trains et de nombreux métros, parfois pendant plus de dix heures.

Les ascenseurs se sont arrêtés, piégeant des centaines de personnes.

Les embouteillages ont paralysé les grandes villes, aggravés par l'arrêt des feux de signalisation.

Les transports publics urbains étaient à l'arrêt, compliquant l'accès aux soins et aux services essentiels.



👉Coupure des communications

Le blackout a provoqué l'arrêt généralisé des réseaux téléphoniques et d'Internet, isolant des millions de personnes.

L'impossibilité de contacter les secours ou de s'informer a accentué le sentiment d'angoisse et rendu la gestion de crise plus difficile.

👉 Arrêt des services d'urgence et médicaux

Les hôpitaux ont fonctionné grâce à des générateurs de secours, mais de nombreux traitements non urgents ont été annulés.

Les patients à domicile, dépendants de dispositifs électriques, se sont retrouvés en situation critique.

Les centres d'accueil temporaires ont été ouverts dans les gares et aéroports pour accueillir les personnes bloquées.

👉 Vie quotidienne et économie paralysées

La privation d'électricité a touché près de 55 millions de personnes.

Les commerces, bars, restaurants et stations-service ont fermé temporairement.

Les paiements électroniques et les distributeurs automatiques de billets étaient hors service, provoquant une ruée sur les produits essentiels (lampes, piles, bougies, denrées alimentaires).

👉 Répercussions internationales

Si la France n'a été que marginalement touchée (quelques foyers au Pays basque), le Maroc a connu des perturbations Internet, et le Groenland**(1)** a temporairement perdu ses moyens de communication gérés depuis l'Espagne.

Cela souligne l'interconnexion croissante des réseaux électriques et numériques à l'échelle internationale.

Origine de la panne : une enquête toujours en cours

La panne résulte d'un enchaînement d'incidents techniques sur le réseau électrique ibérique, aggravés par une forte dépendance aux énergies renouvelables et un manque de réserve thermique.

Les investigations ont écarté la cyberattaque et les phénomènes atmosphériques comme causes principales. La coupure s'est propagée rapidement en raison de protections automatiques et d'interconnexions fragiles.

L'origine est donc multifactorielle et structurelle.

Cette crise souligne l'urgence de renforcer la résilience et l'anticipation dans la gestion des réseaux électriques.

La coordination européenne a permis d'éviter une propagation plus large de la panne, mais l'événement reste sans précédent par son ampleur et sa soudaineté.

(1) https://www.tf1info.fr/international/en-direct-coupure-de-courant-massive-l-espagne-et-le-portugal-france-narbonne-perpignan-prives-d-electricite-depuis-12h30-2367599.html

Gestion de crise et enseignements

L'état d'urgence a été déclenché, les plans de continuité et de reprise d'activité ont été activés, et la priorité a été donnée au rétablissement des infrastructures critiques.

Cette crise a révélé la nécessité de :

- Renforcer la résilience des réseaux électriques
- Mieux protéger les personnes vulnérables
- Améliorer la communication de crise
- Sensibiliser la population à la préparation individuelle face aux risques majeurs.

Cette crise souligne l'importance d'une approche globale et proactive, combinant innovation technologique, organisation efficace et culture du risque partagée, pour garantir la continuité d'alimentation électrique face aux défis actuels et futurs.

Ce blackout historique restera dans les mémoires comme un signal d'alarme pour l'ensemble des pays européens.

Il rappelle l'importance de la gestion de crise, de la continuité d'activité et de la préparation collective et individuelle.

Les leçons tirées de cet événement devront guider les politiques publiques et les stratégies des entreprises pour faire face à des risques systémiques de plus en plus fréquents dans un monde interconnecté.

Alexandre Fournier

Préparez-vous...

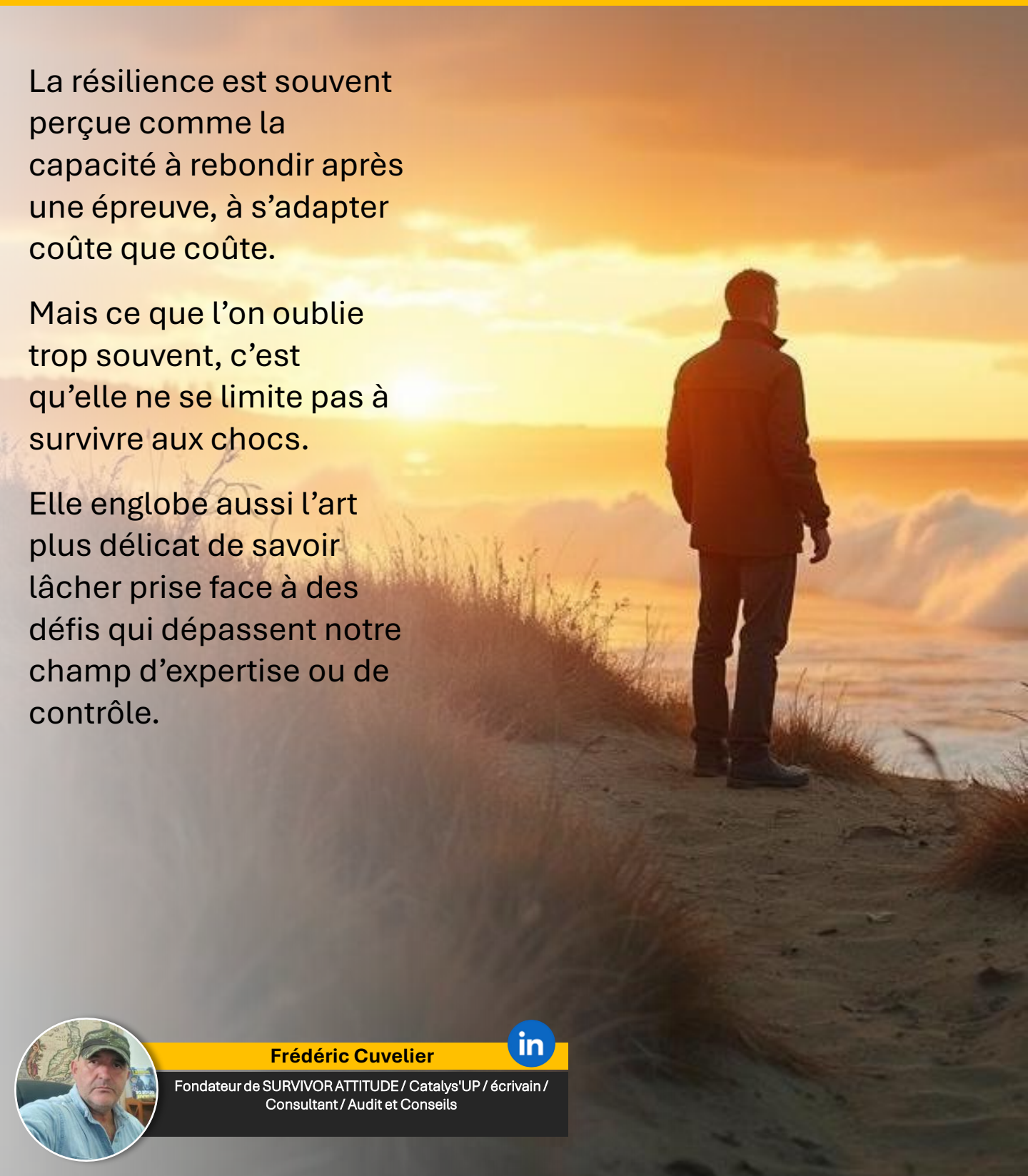
Conférence – Juillet 2024

Exercice de crise – Mars 2025

Interview – Mai 2025

Dossier Spécial – Octobre 2024

Résilience : Entre adaptation et lâcher-prise, une danse subtile pour évoluer



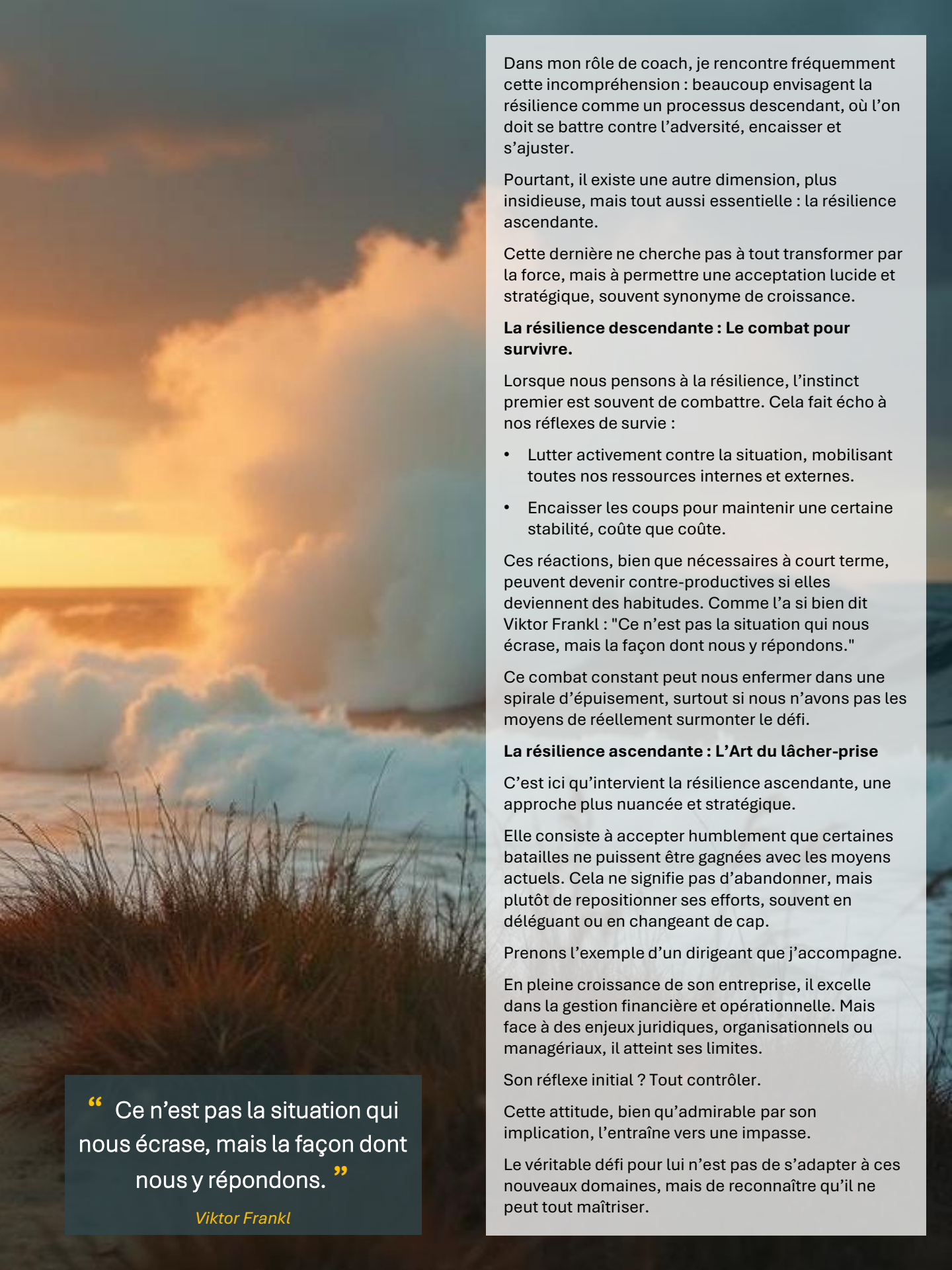
La résilience est souvent perçue comme la capacité à rebondir après une épreuve, à s'adapter coûte que coûte.

Mais ce que l'on oublie trop souvent, c'est qu'elle ne se limite pas à survivre aux chocs.

Elle englobe aussi l'art plus délicat de savoir lâcher prise face à des défis qui dépassent notre champ d'expertise ou de contrôle.

Frédéric Cuvelier

Fondateur de SURVIVOR ATTITUDE / Catalys'UP / écrivain / Consultant / Audit et Conseils



Dans mon rôle de coach, je rencontre fréquemment cette incompréhension : beaucoup envisagent la résilience comme un processus descendant, où l'on doit se battre contre l'adversité, encaisser et s'ajuster.

Pourtant, il existe une autre dimension, plus insidieuse, mais tout aussi essentielle : la résilience ascendante.

Cette dernière ne cherche pas à tout transformer par la force, mais à permettre une acceptation lucide et stratégique, souvent synonyme de croissance.

La résilience descendante : Le combat pour survivre.

Lorsque nous pensons à la résilience, l'instinct premier est souvent de combattre. Cela fait écho à nos réflexes de survie :

- Lutter activement contre la situation, mobilisant toutes nos ressources internes et externes.
- Encaisser les coups pour maintenir une certaine stabilité, coûte que coûte.

Ces réactions, bien que nécessaires à court terme, peuvent devenir contre-productives si elles deviennent des habitudes. Comme l'a si bien dit Viktor Frankl : "Ce n'est pas la situation qui nous écrase, mais la façon dont nous y répondons."

Ce combat constant peut nous enfermer dans une spirale d'épuisement, surtout si nous n'avons pas les moyens de réellement surmonter le défi.

La résilience ascendante : L'Art du lâcher-prise

C'est ici qu'intervient la résilience ascendante, une approche plus nuancée et stratégique.

Elle consiste à accepter humblement que certaines batailles ne puissent être gagnées avec les moyens actuels. Cela ne signifie pas d'abandonner, mais plutôt de repositionner ses efforts, souvent en déléguant ou en changeant de cap.

Prenons l'exemple d'un dirigeant que j'accompagne.

En pleine croissance de son entreprise, il excelle dans la gestion financière et opérationnelle. Mais face à des enjeux juridiques, organisationnels ou managériaux, il atteint ses limites.

Son réflexe initial ? Tout contrôler.

Cette attitude, bien qu'admirable par son implication, l'entraîne vers une impasse.

Le véritable défi pour lui n'est pas de s'adapter à ces nouveaux domaines, mais de reconnaître qu'il ne peut tout maîtriser.

> “ Ce n'est pas la situation qui nous écrase, mais la façon dont nous y répondons. ”
>
> *Viktor Frankl*

Mon rôle consiste à l'accompagner dans un lâcher-prise stratégique : accepter qu'il ne puisse s'adapter à tout, déléguer les responsabilités adéquates et se concentrer sur ses points forts.

Les Trois Postures de la Résilience.

Dans un contexte de survie, trois postures fondamentales s'offrent à nous :

1. **Combattre :** Utiliser ses forces pour surmonter l'obstacle.
2. **Fuir :** Prendre du recul, contourner le problème ou le reporter.
3. **Inhiber :** Faire une pause stratégique pour préserver ses ressources.

La clé de la résilience parfaite réside dans la capacité à choisir la bonne posture au bon moment.

Combattre n'est pas toujours
la meilleure option.

Parfois, reculer ou s'arrêter permet de mieux avancer par la suite.

Comme le dit Lao Tseu : "*L'eau est fluide, douce et malléable. Mais l'eau érode le roc, qui est rigide et résistant. Ce qui est souple est plus fort que ce qui est dur.*"

Cette citation illustre la puissance du lâcher-prise.

Un Processus structuré pour une résilience durable

Que ce soit dans la résilience descendante ou ascendante, un processus méthodique est indispensable :

1. **Encaisser :** Reconnaître et absorber l'impact émotionnel et situationnel.
2. **Temporiser :** Prendre du recul pour éviter les décisions impulsives.
3. **Analyser :** Identifier les leviers d'action disponibles.
4. **Choisir :** Déterminer la posture (combat, fuite ou inhibition) la plus adaptée.
5. **Fixer des objectifs jalonnés :** Définir un plan d'action clair et mesurable.
6. **Évaluer régulièrement :** Ajuster le cap selon les résultats obtenus.

Ce processus permet de transformer une réaction instinctive en une réponse stratégique, que ce soit pour résister ou pour lâcher prise.

> "L'eau est fluide, douce et malléable. Mais l'eau érode le roc, qui est rigide et résistant. Ce qui est souple est plus fort que ce qui est dur."
>
> *Lao Tseu*

Résilience et évolution : un équilibre essentiel

La résilience est donc bien plus qu'une simple capacité à s'adapter.

Elle est une danse subtile entre résistance et flexibilité, où chaque étape demande une introspection et une stratégie adaptées au contexte.

Face à un défi, posez-vous cette question essentielle :

"Est-il temps de combattre,

de reculer ou de lâcher prise ?"

La réponse à cette question déterminera non seulement votre capacité à surmonter l'épreuve, mais aussi à évoluer durablement.

En entreprise comme dans la vie, savoir lâcher prise n'est pas une faiblesse, mais une force stratégique, un acte de résilience ascendante qui ouvre la voie à une transformation positive et pérenne.

Conclusion :

Résister, reculer, lâcher-prise : La trilogie de la résilience stratégique. Face aux défis constants du monde professionnel, il est temps de repenser notre manière de répondre à l'adversité. Plutôt que de s'enfermer dans des réflexes primaires, tels que combattre, fuir ou s'immobiliser, je propose une nouvelle approche : la résilience stratégique.

Frédéric CUVELIER

Mon parcours, forgé dans des environnements extrêmes, m'a enseigné que la résilience et l'autonomie sont des piliers essentiels face aux imprévus. Contrairement à d'autres experts bénéficiant d'un soutien logistique conséquent, j'ai acquis la capacité de planifier, exécuter et gérer des missions complexes en totale indépendance. Ces compétences me permettent de transmettre des savoir-faire concrets et adaptés à travers des formations et des audits en sécurité et en gestion des crises.

https://www.survivorattitude.com

Cette méthode

Repose sur trois piliers stratégiques, qui offrent une réponse lucide et structurée à l'incertitude :

1. **Résister :** Utiliser toutes ses ressources pour faire face à une situation critique et maintenir le cap malgré les turbulences.
2. **Reculer :** S'accorder le temps nécessaire pour analyser une situation avec une perspective élargie, afin de planifier des actions plus réfléchies et efficaces.
3. **Lâcher prise :** Savoir céder le contrôle sur des aspects secondaires ou inaccessibles, et reconnaître que la délégation ou l'acceptation peuvent être des leviers puissants pour atteindre des solutions pérennes.

Cette approche transcende la simple survie.

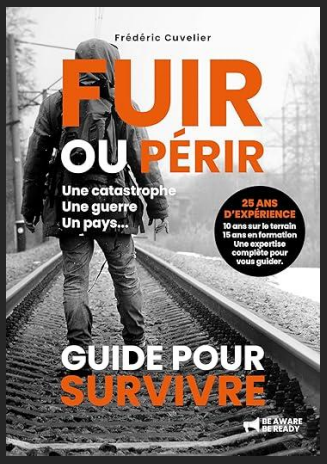
Elle repose sur un équilibre dynamique, où chaque posture est choisie en fonction des circonstances.

Comme l'affirme si justement une grande vérité :

"La vraie force résiliente ne consiste pas seulement à combattre l'adversité, mais à savoir quand il est plus judicieux de reculer pour mieux avancer, ou de lâcher prise pour ouvrir de nouvelles opportunités."

Avec cette résilience puissante, l'entreprise ne se contente plus de subir les aléas : elle devient actrice de son propre avenir, prête à transformer chaque obstacle en un levier de progression durable.

À LIRE *DU MÊME AUTEUR ...*



La Web radio
Crise & Résilience

L'unique WebRadio qui
Renforce votre Cyber Résilience,
un épisode à la fois

À ÉCOUTEZ ICI

www.radiocriseetresilience.com

Code QR de la WebRadio

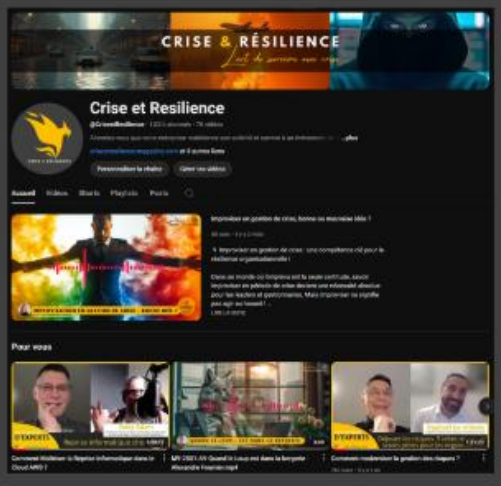
La chaîne youtube Crise & Résilience

L'unique chaîne Youtube qui

Renforce votre Cyber Résilience,

une vidéo à la fois

À REGARDEZ ICI



Code QR de Youtube

www.youtube.com/criseetresilience

Cyberattaque sur Promptis .Inc

C’est toi le héros de cette histoire !

Vous allez incarner Alex Martin, responsable de la gestion de crise au sein de l’entreprise Promptis .Inc.

Cette PME dynamique de 150 salariés est spécialisée dans le développement de solutions logicielles d’intelligence artificielle pour le secteur médical.

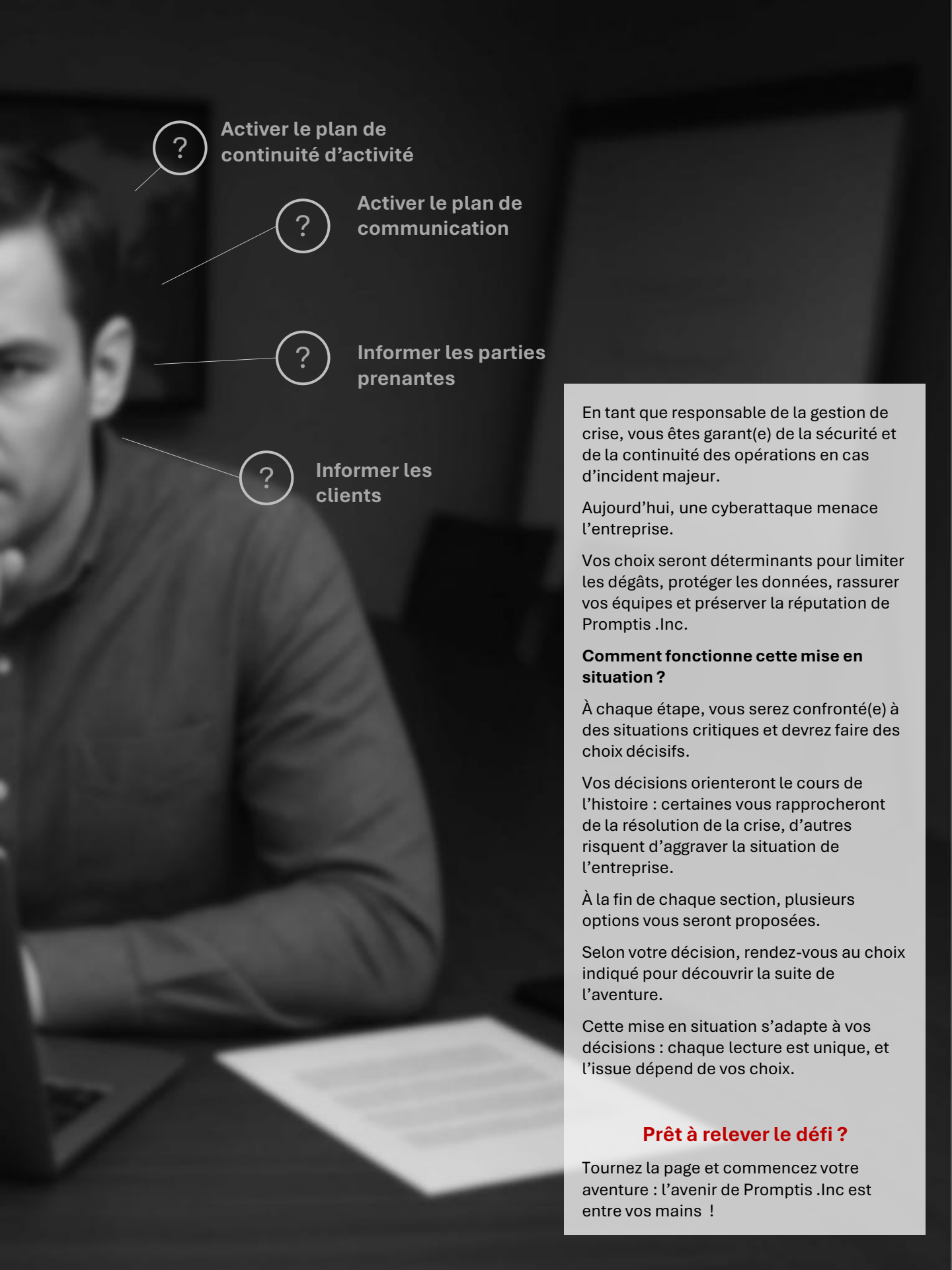
L’entreprise gère des données sensibles, travaille avec des hôpitaux et des laboratoires, et dépend fortement de ses systèmes informatiques pour assurer son activité quotidienne.

Votre avis est important pour nous.

Merci de répondre à ce questionnaire à la fin...

Karine Maréchal-Richard

Experte en continuité des affaires et en gestion de crise
Consultante, formatrice et conférencière dans les domaines de la continuité des affaires et de la gestion de crise.



En tant que responsable de la gestion de crise, vous êtes garant(e) de la sécurité et de la continuité des opérations en cas d'incident majeur.

Aujourd'hui, une cyberattaque menace l'entreprise.

Vos choix seront déterminants pour limiter les dégâts, protéger les données, rassurer vos équipes et préserver la réputation de Promptis .Inc.

Comment fonctionne cette mise en situation ?

À chaque étape, vous serez confronté(e) à des situations critiques et devrez faire des choix décisifs.

Vos décisions orienteront le cours de l'histoire : certaines vous rapprocheront de la résolution de la crise, d'autres risquent d'aggraver la situation de l'entreprise.

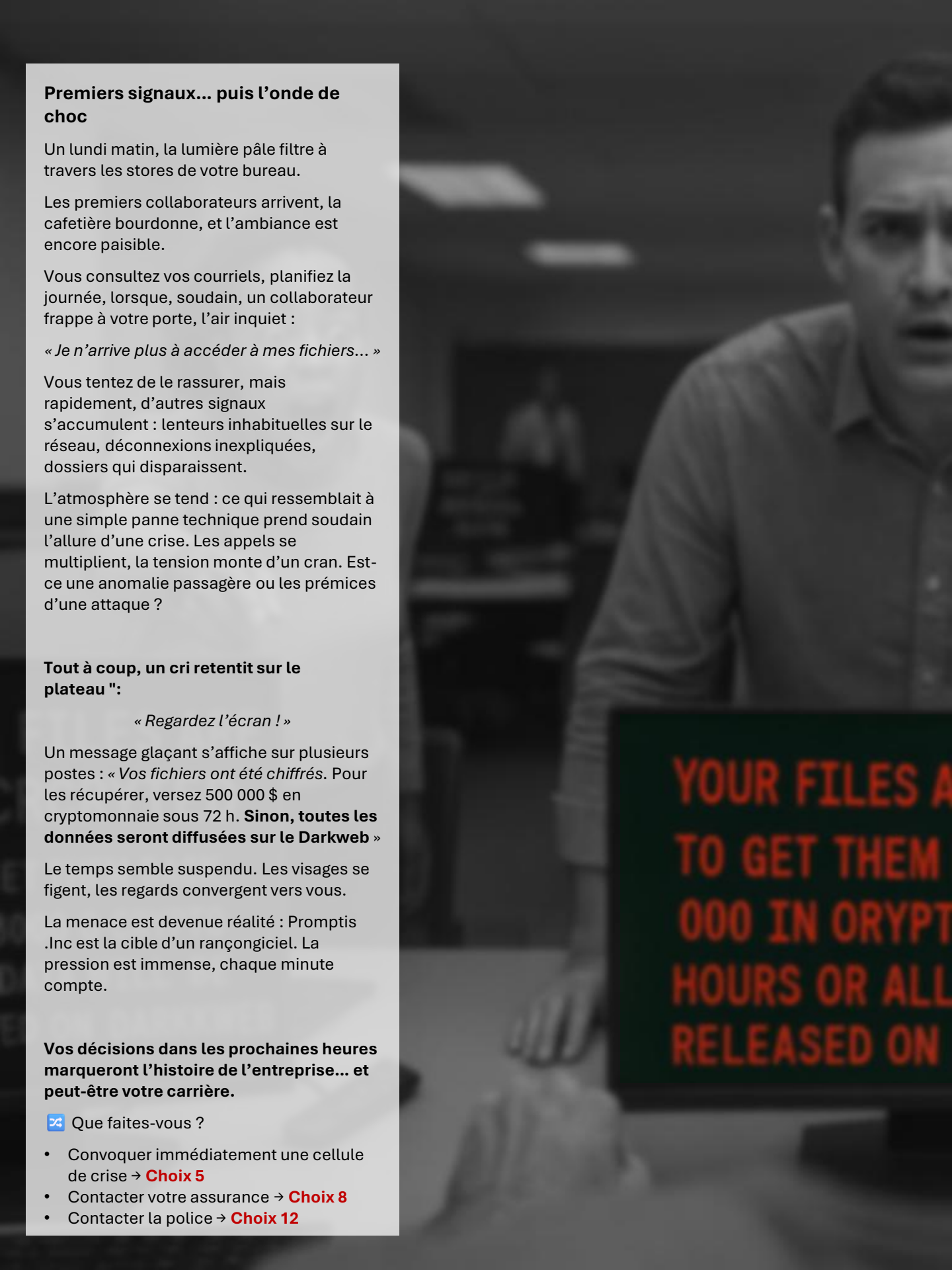
À la fin de chaque section, plusieurs options vous seront proposées.

Selon votre décision, rendez-vous au choix indiqué pour découvrir la suite de l'aventure.

Cette mise en situation s'adapte à vos décisions : chaque lecture est unique, et l'issue dépend de vos choix.

Prêt à relever le défi ?

Tournez la page et commencez votre aventure : l'avenir de Promptis .Inc est entre vos mains !



Premiers signaux… puis l'onde de choc

Un lundi matin, la lumière pâle filtre à travers les stores de votre bureau.

Les premiers collaborateurs arrivent, la cafetière bourdonne, et l'ambiance est encore paisible.

Vous consultez vos courriels, planifiez la journée, lorsque, soudain, un collaborateur frappe à votre porte, l'air inquiet :

« Je n'arrive plus à accéder à mes fichiers… »

Vous tentez de le rassurer, mais rapidement, d'autres signaux s'accumulent : lenteurs inhabituelles sur le réseau, déconnexions inexpliquées, dossiers qui disparaissent.

L'atmosphère se tend : ce qui ressemblait à une simple panne technique prend soudain l'allure d'une crise. Les appels se multiplient, la tension monte d'un cran. Est-ce une anomalie passagère ou les prémices d'une attaque ?

Tout à coup, un cri retentit sur le plateau ":

« Regardez l'écran ! »

Un message glaçant s'affiche sur plusieurs postes : *« Vos fichiers ont été chiffrés.* Pour les récupérer, versez 500 000 $ en cryptomonnaie sous 72 h. **Sinon, toutes les données seront diffusées sur le Darkweb** »

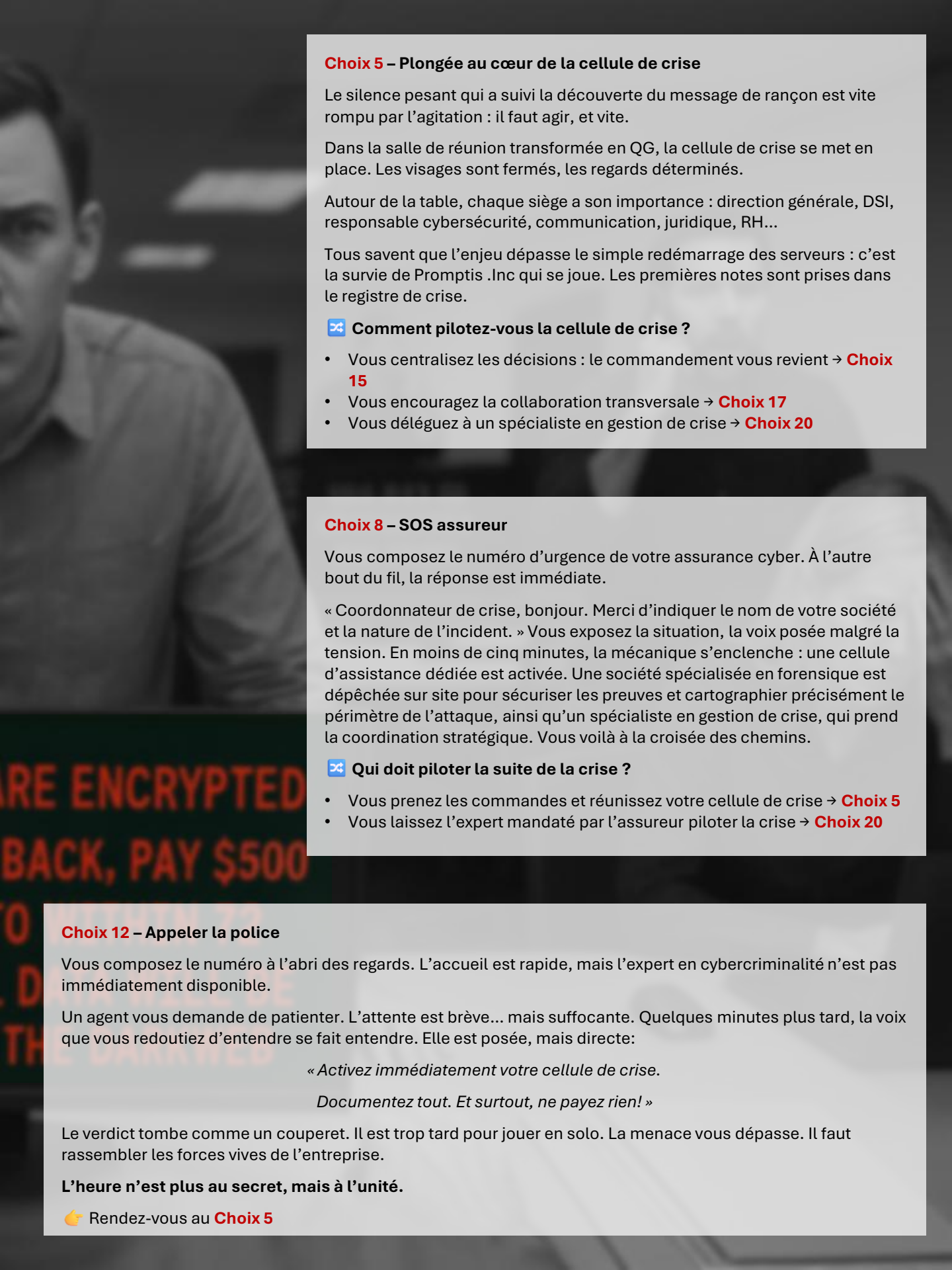
Le temps semble suspendu. Les visages se figent, les regards convergent vers vous.

La menace est devenue réalité : Promptis .Inc est la cible d'un rançongiciel. La pression est immense, chaque minute compte.

Vos décisions dans les prochaines heures marqueront l'histoire de l'entreprise… et peut-être votre carrière.

🔀 Que faites-vous ?

- Convoquer immédiatement une cellule de crise → **Choix 5**
- Contacter votre assurance → **Choix 8**
- Contacter la police → **Choix 12**



Choix 5 – Plongée au cœur de la cellule de crise

Le silence pesant qui a suivi la découverte du message de rançon est vite rompu par l'agitation : il faut agir, et vite.

Dans la salle de réunion transformée en QG, la cellule de crise se met en place. Les visages sont fermés, les regards déterminés.

Autour de la table, chaque siège a son importance : direction générale, DSI, responsable cybersécurité, communication, juridique, RH…

Tous savent que l'enjeu dépasse le simple redémarrage des serveurs : c'est la survie de Promptis .Inc qui se joue. Les premières notes sont prises dans le registre de crise.

🔀 **Comment pilotez-vous la cellule de crise ?**

- Vous centralisez les décisions : le commandement vous revient → **Choix 15**
- Vous encouragez la collaboration transversale → **Choix 17**
- Vous déléguez à un spécialiste en gestion de crise → **Choix 20**

Choix 8 – SOS assureur

Vous composez le numéro d'urgence de votre assurance cyber. À l'autre bout du fil, la réponse est immédiate.

« Coordonnateur de crise, bonjour. Merci d'indiquer le nom de votre société et la nature de l'incident. » Vous exposez la situation, la voix posée malgré la tension. En moins de cinq minutes, la mécanique s'enclenche : une cellule d'assistance dédiée est activée. Une société spécialisée en forensique est dépêchée sur site pour sécuriser les preuves et cartographier précisément le périmètre de l'attaque, ainsi qu'un spécialiste en gestion de crise, qui prend la coordination stratégique. Vous voilà à la croisée des chemins.

🔀 **Qui doit piloter la suite de la crise ?**

- Vous prenez les commandes et réunissez votre cellule de crise → **Choix 5**
- Vous laissez l'expert mandaté par l'assureur piloter la crise → **Choix 20**

Choix 12 – Appeler la police

Vous composez le numéro à l'abri des regards. L'accueil est rapide, mais l'expert en cybercriminalité n'est pas immédiatement disponible.

Un agent vous demande de patienter. L'attente est brève… mais suffocante. Quelques minutes plus tard, la voix que vous redoutiez d'entendre se fait entendre. Elle est posée, mais directe:

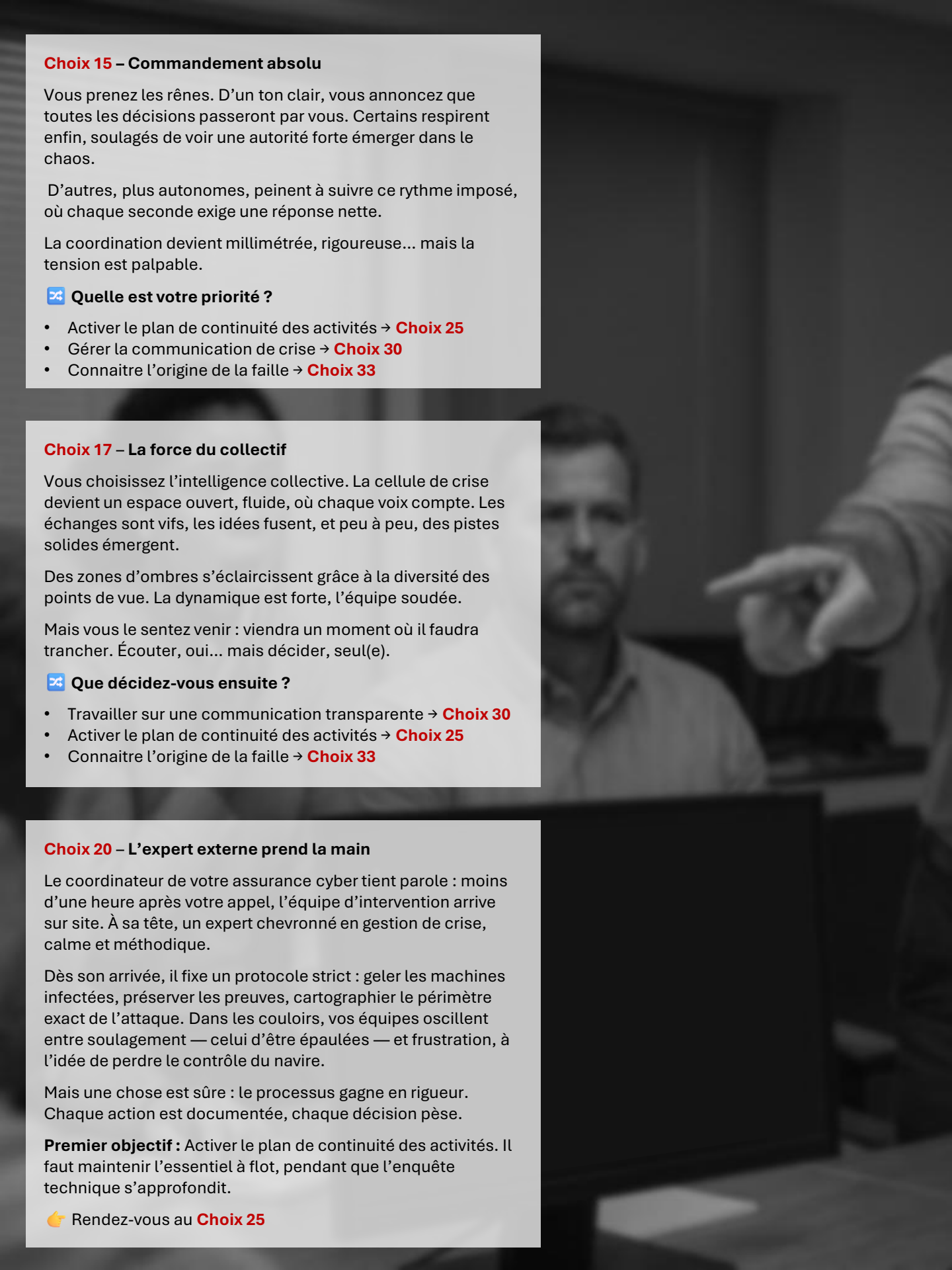
« Activez immédiatement votre cellule de crise.

Documentez tout. Et surtout, ne payez rien! »

Le verdict tombe comme un couperet. Il est trop tard pour jouer en solo. La menace vous dépasse. Il faut rassembler les forces vives de l'entreprise.

L'heure n'est plus au secret, mais à l'unité.

👉 Rendez-vous au **Choix 5**



Choix 15 – Commandement absolu

Vous prenez les rênes. D'un ton clair, vous annoncez que toutes les décisions passeront par vous. Certains respirent enfin, soulagés de voir une autorité forte émerger dans le chaos.

D'autres, plus autonomes, peinent à suivre ce rythme imposé, où chaque seconde exige une réponse nette.

La coordination devient millimétrée, rigoureuse… mais la tension est palpable.

🔀 **Quelle est votre priorité ?**

- Activer le plan de continuité des activités → **Choix 25**
- Gérer la communication de crise → **Choix 30**
- Connaitre l'origine de la faille → **Choix 33**

Choix 17 – La force du collectif

Vous choisissez l'intelligence collective. La cellule de crise devient un espace ouvert, fluide, où chaque voix compte. Les échanges sont vifs, les idées fusent, et peu à peu, des pistes solides émergent.

Des zones d'ombres s'éclaircissent grâce à la diversité des points de vue. La dynamique est forte, l'équipe soudée.

Mais vous le sentez venir : viendra un moment où il faudra trancher. Écouter, oui… mais décider, seul(e).

🔀 **Que décidez-vous ensuite ?**

- Travailler sur une communication transparente → **Choix 30**
- Activer le plan de continuité des activités → **Choix 25**
- Connaitre l'origine de la faille → **Choix 33**

Choix 20 – L'expert externe prend la main

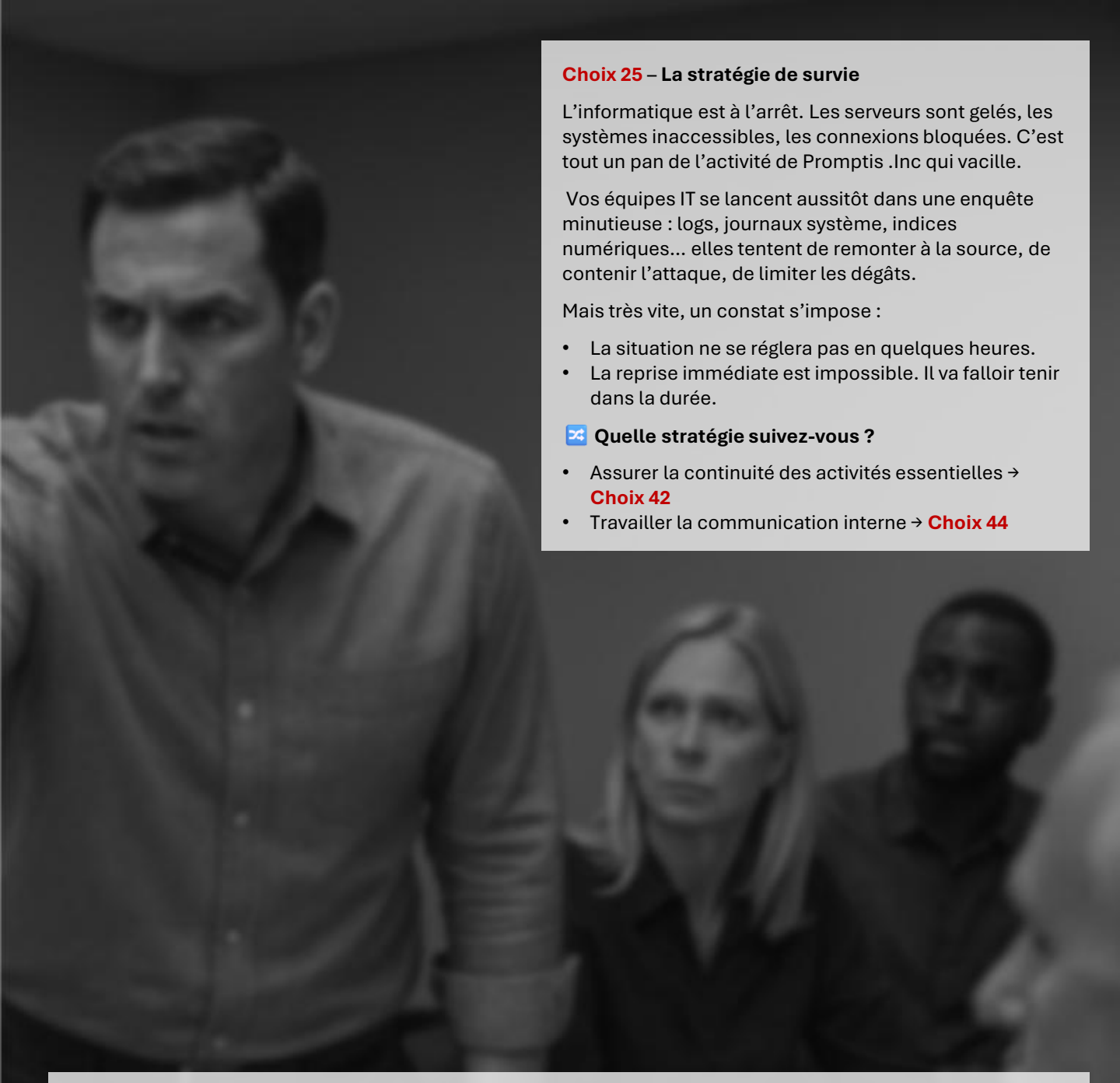
Le coordinateur de votre assurance cyber tient parole : moins d'une heure après votre appel, l'équipe d'intervention arrive sur site. À sa tête, un expert chevronné en gestion de crise, calme et méthodique.

Dès son arrivée, il fixe un protocole strict : geler les machines infectées, préserver les preuves, cartographier le périmètre exact de l'attaque. Dans les couloirs, vos équipes oscillent entre soulagement — celui d'être épaulées — et frustration, à l'idée de perdre le contrôle du navire.

Mais une chose est sûre : le processus gagne en rigueur. Chaque action est documentée, chaque décision pèse.

Premier objectif : Activer le plan de continuité des activités. Il faut maintenir l'essentiel à flot, pendant que l'enquête technique s'approfondit.

👉 Rendez-vous au **Choix 25**



Choix 25 – **La stratégie de survie**

L'informatique est à l'arrêt. Les serveurs sont gelés, les systèmes inaccessibles, les connexions bloquées. C'est tout un pan de l'activité de Promptis .Inc qui vacille.

Vos équipes IT se lancent aussitôt dans une enquête minutieuse : logs, journaux système, indices numériques… elles tentent de remonter à la source, de contenir l'attaque, de limiter les dégâts.

Mais très vite, un constat s'impose :

- La situation ne se réglera pas en quelques heures.
- La reprise immédiate est impossible. Il va falloir tenir dans la durée.

🔀 **Quelle stratégie suivez-vous ?**

- Assurer la continuité des activités essentielles → **Choix 42**
- Travailler la communication interne → **Choix 44**

Choix 30 – **Sous pression : choisir les bons mots**

Le téléphone n'arrête plus de sonner. Les clients exigent des explications. Les salariés cherchent des repères.

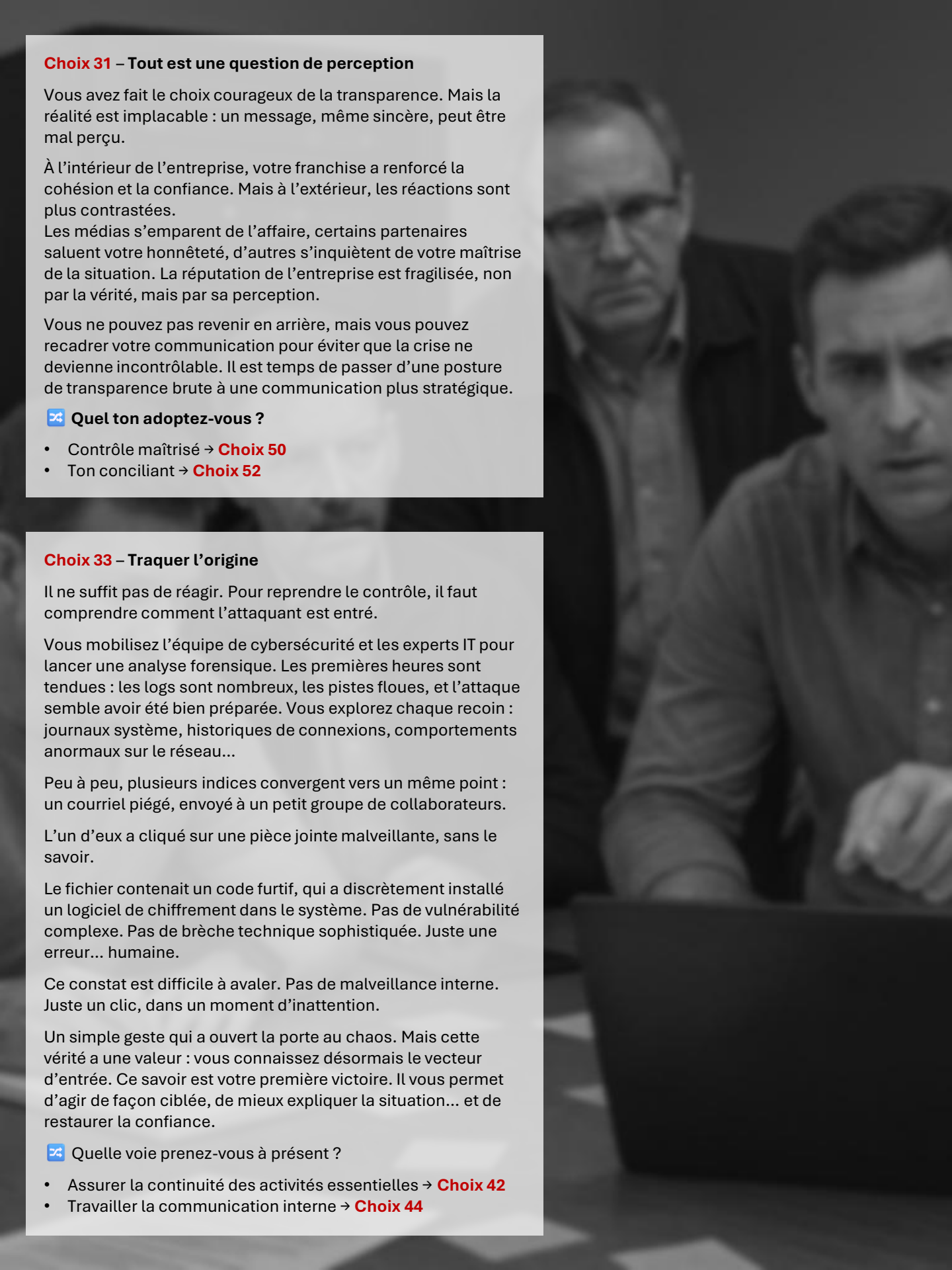
Dans cette cacophonie grandissante, chaque mot prononcé, chaque message diffusé, chaque minute de silence devient une décision stratégique.

Un mot mal pesé peut semer la panique. Une phrase mal formulée peut décrédibiliser toute votre réponse. Vous n'avez plus le luxe du silence.

Il est temps de communiquer. Mais avec quel ton ? Et dans quel cadre ?

🔀 **Quel ton adoptez-vous ?**

- Transparence totale → **Choix 47**
- Contrôle maîtrisé → **Choix 50**
- Ton conciliant → **Choix 52**



Choix 31 – **Tout est une question de perception**

Vous avez fait le choix courageux de la transparence. Mais la réalité est implacable : un message, même sincère, peut être mal perçu.

À l'intérieur de l'entreprise, votre franchise a renforcé la cohésion et la confiance. Mais à l'extérieur, les réactions sont plus contrastées.
Les médias s'emparent de l'affaire, certains partenaires saluent votre honnêteté, d'autres s'inquiètent de votre maîtrise de la situation. La réputation de l'entreprise est fragilisée, non par la vérité, mais par sa perception.

Vous ne pouvez pas revenir en arrière, mais vous pouvez recadrer votre communication pour éviter que la crise ne devienne incontrôlable. Il est temps de passer d'une posture de transparence brute à une communication plus stratégique.

🔀 **Quel ton adoptez-vous ?**

- Contrôle maîtrisé → **Choix 50**
- Ton conciliant → **Choix 52**

Choix 33 – **Traquer l'origine**

Il ne suffit pas de réagir. Pour reprendre le contrôle, il faut comprendre comment l'attaquant est entré.

Vous mobilisez l'équipe de cybersécurité et les experts IT pour lancer une analyse forensique. Les premières heures sont tendues : les logs sont nombreux, les pistes floues, et l'attaque semble avoir été bien préparée. Vous explorez chaque recoin : journaux système, historiques de connexions, comportements anormaux sur le réseau…

Peu à peu, plusieurs indices convergent vers un même point : un courriel piégé, envoyé à un petit groupe de collaborateurs.

L'un d'eux a cliqué sur une pièce jointe malveillante, sans le savoir.

Le fichier contenait un code furtif, qui a discrètement installé un logiciel de chiffrement dans le système. Pas de vulnérabilité complexe. Pas de brèche technique sophistiquée. Juste une erreur… humaine.

Ce constat est difficile à avaler. Pas de malveillance interne. Juste un clic, dans un moment d'inattention.

Un simple geste qui a ouvert la porte au chaos. Mais cette vérité a une valeur : vous connaissez désormais le vecteur d'entrée. Ce savoir est votre première victoire. Il vous permet d'agir de façon ciblée, de mieux expliquer la situation… et de restaurer la confiance.

🔀 Quelle voie prenez-vous à présent ?

- Assurer la continuité des activités essentielles → **Choix 42**
- Travailler la communication interne → **Choix 44**

Choix 42 – **Cap sur l'essentiel**

Les équipes appliquent les procédures prévues dans le Plan de Continuité des Activités.

Là où les outils numériques sont inaccessibles, des méthodes alternatives prennent le relais : papier, téléphone, coordination manuelle.

C'est loin d'être idéal… mais ça fonctionne.

L'organisation tourne en mode dégradé, les activités essentielles sont maintenues. Vous avez réussi à contenir l'effondrement, à sécuriser l'essentiel.

Une première victoire!

👉 Rendez-vous au → **Choix 60**

Choix 44 – **Préserver l'humain au cœur de la crise**

Dans la tourmente, vous choisissez de ne pas négliger l'élément le plus fragile… et le plus précieux : les équipes. Car si les systèmes tombent, la communication, elle, peut – et doit – tenir bon.

Vous activez votre plan de communication – volet interne. Des points réguliers sont instaurés avec les directeurs.

Les salariés sont tenus informés de l'évolution de la situation, des décisions prises, des efforts en cours. Les rumeurs sont étouffées et les tensions désamorcées.

Vous donnez du sens à l'incertitude.

Résultat : le stress recule, la cohésion se renforce, et les collaborateurs deviennent partie prenante de la résilience collective. Grâce à cette stabilité humaine, vous avez gagné une chose que peu d'outils peuvent offrir : la mobilisation.

👉 Il est temps de choisir, rendez-vous au → **Choix 60**

Choix 47 – **Transparence totale**

Votre message est clair, assumé, sans détour. Vous faites le choix courageux de la transparence totale, exposant les faits, reconnaissant la gravité de l'attaque, sans chercher à en atténuer l'impact.

Mais cette sincérité a un prix.

Les partenaires vous remercient pour votre honnêteté, les équipes se serrent les coudes, galvanisés par votre franchise. En interne, la cohésion renaît.

Mais à l'extérieur, le regard change. Les médias s'emparent de l'affaire.

Si certains saluent votre courage, d'autres dénoncent une faille majeure dans la gouvernance numérique, une négligence en matière de cybersécurité. Le nom de votre entreprise fait les gros titres… pas pour de bonnes raisons.

L'image de Promptis .Inc est écornée. Votre intégrité n'est pas remise en cause, mais la confiance de certains clients vacille. Le doute s'installe dans les esprits. La réputation, elle, ne se restaure pas en un communiqué.

👉 Réévaluez votre stratégie de communication → **Choix 31**

Choix 50 – Le juste milieu

Votre communication est mesurée, stratégique

Vous choisissez le juste milieu : dire l'essentiel, sans provoquer de panique. Pas de dramatisation, pas de langue de bois non plus.

Le message est clair, cadré, et donne une impression de maîtrise.

La situation semble sous contrôle — du moins en surface. Les équipes sont rassurées, les clients restent vigilants.

Mais dans ce silence relatif, certains s'interrogent : que cache-t-on ? Jusqu'où la crise s'étend-elle vraiment ?

Vous avez gagné du temps… mais pas encore la confiance totale.

Vous ne pouvez plus attendre. Il est temps d'assurer la continuité des opérations vitales, même en mode dégradé.

👉 Rendez-vous au **Choix 42**

Choix 52 – Trop positif… Trop tard

Vous choisissez d'adopter un ton conciliant, espérant apaiser les tensions et préserver l'image de l'entreprise. Votre message met en avant la mobilisation des équipes et la volonté de rétablir la situation rapidement.

Mais le ton est trop léger… et cela ne passe pas.

Les clients ne sont pas dupes. Les incohérences, les silences, les formules vagues — tout cela soulève des questions. Les employés, eux aussi, doutent. Dans les couloirs, les conversations deviennent plus tendues. On cherche des réponses que votre message n'a pas données.

Ce qui devait calmer les esprits finit par semer la confusion. La crédibilité vacille. Et dans une crise, c'est parfois ce qu'on perd en premier. Perte de crédibilité.

👉 Reprenez la main avec une communication plus maîtrisée → **Choix 50**

Choix 60 – L'ultimatum

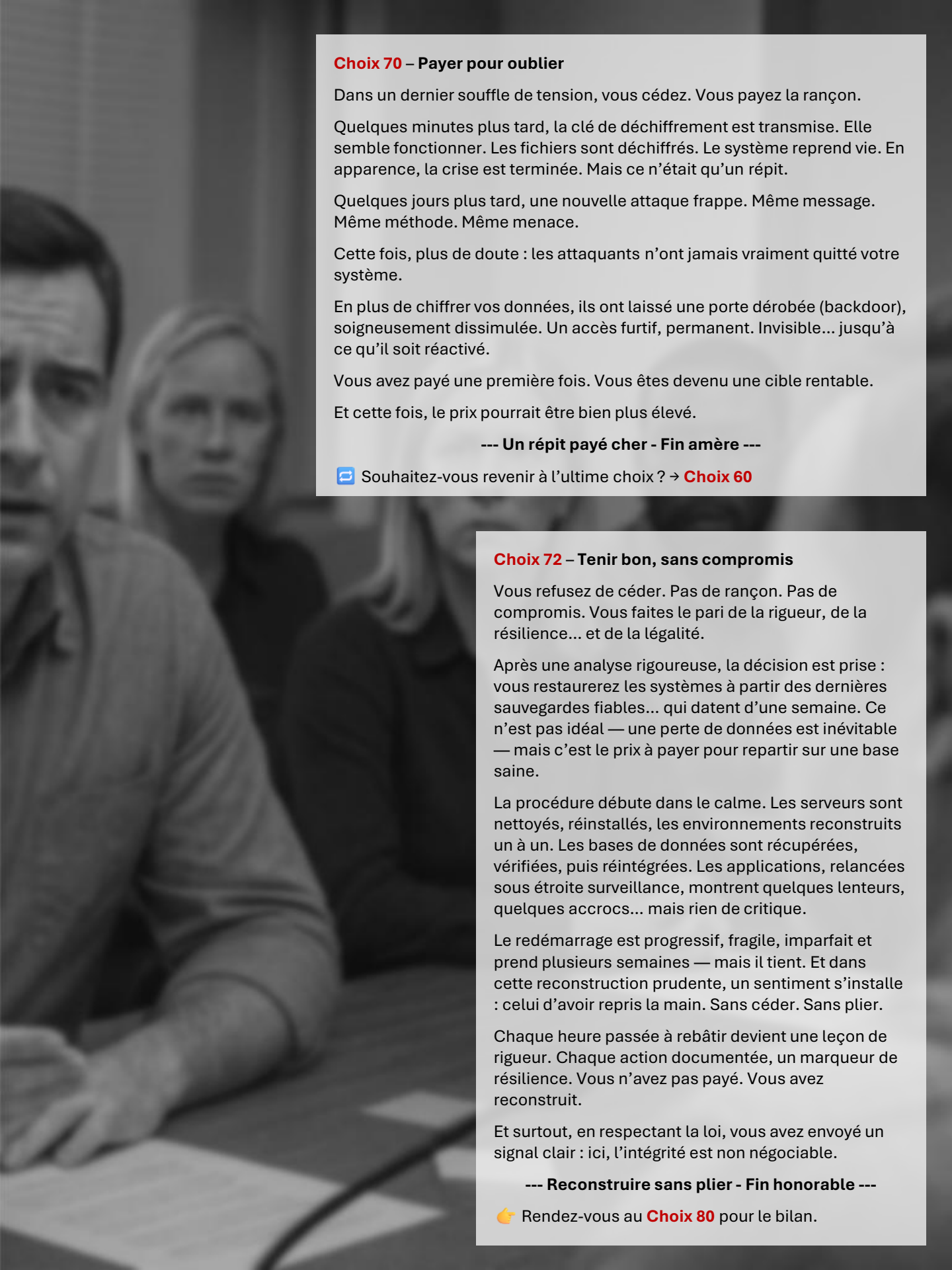
23h59. Le silence est pesant, coupé seulement par le bourdonnement des machines de secours et les regards épuisés autour de vous.

Le message de rançon clignote encore sur certains écrans, comme un compte à rebours oppressant. Dans une minute, il sera trop tard.

Les équipes vous regardent. Les autorités attendent votre décision. Les nerfs sont à vif. Il ne reste plus qu'une question, suspendue dans l'air comme une lame : que faire ?

🔀 **Quelle voie choisissez-vous ?**

- Payer discrètement la rançon → **Choix 70**
- Restaurer à partir des sauvegardes → **Choix 72**
- Travailler avec un cabinet externe et médiatisé → **Choix 75**



Choix 70 – **Payer pour oublier**

Dans un dernier souffle de tension, vous cédez. Vous payez la rançon.

Quelques minutes plus tard, la clé de déchiffrement est transmise. Elle semble fonctionner. Les fichiers sont déchiffrés. Le système reprend vie. En apparence, la crise est terminée. Mais ce n'était qu'un répit.

Quelques jours plus tard, une nouvelle attaque frappe. Même message. Même méthode. Même menace.

Cette fois, plus de doute : les attaquants n'ont jamais vraiment quitté votre système.

En plus de chiffrer vos données, ils ont laissé une porte dérobée (backdoor), soigneusement dissimulée. Un accès furtif, permanent. Invisible… jusqu'à ce qu'il soit réactivé.

Vous avez payé une première fois. Vous êtes devenu une cible rentable.

Et cette fois, le prix pourrait être bien plus élevé.

--- Un répit payé cher - Fin amère ---

🔁 Souhaitez-vous revenir à l'ultime choix ? → **Choix 60**

Choix 72 – **Tenir bon, sans compromis**

Vous refusez de céder. Pas de rançon. Pas de compromis. Vous faites le pari de la rigueur, de la résilience… et de la légalité.

Après une analyse rigoureuse, la décision est prise : vous restaurerez les systèmes à partir des dernières sauvegardes fiables… qui datent d'une semaine. Ce n'est pas idéal — une perte de données est inévitable — mais c'est le prix à payer pour repartir sur une base saine.

La procédure débute dans le calme. Les serveurs sont nettoyés, réinstallés, les environnements reconstruits un à un. Les bases de données sont récupérées, vérifiées, puis réintégrées. Les applications, relancées sous étroite surveillance, montrent quelques lenteurs, quelques accrocs… mais rien de critique.

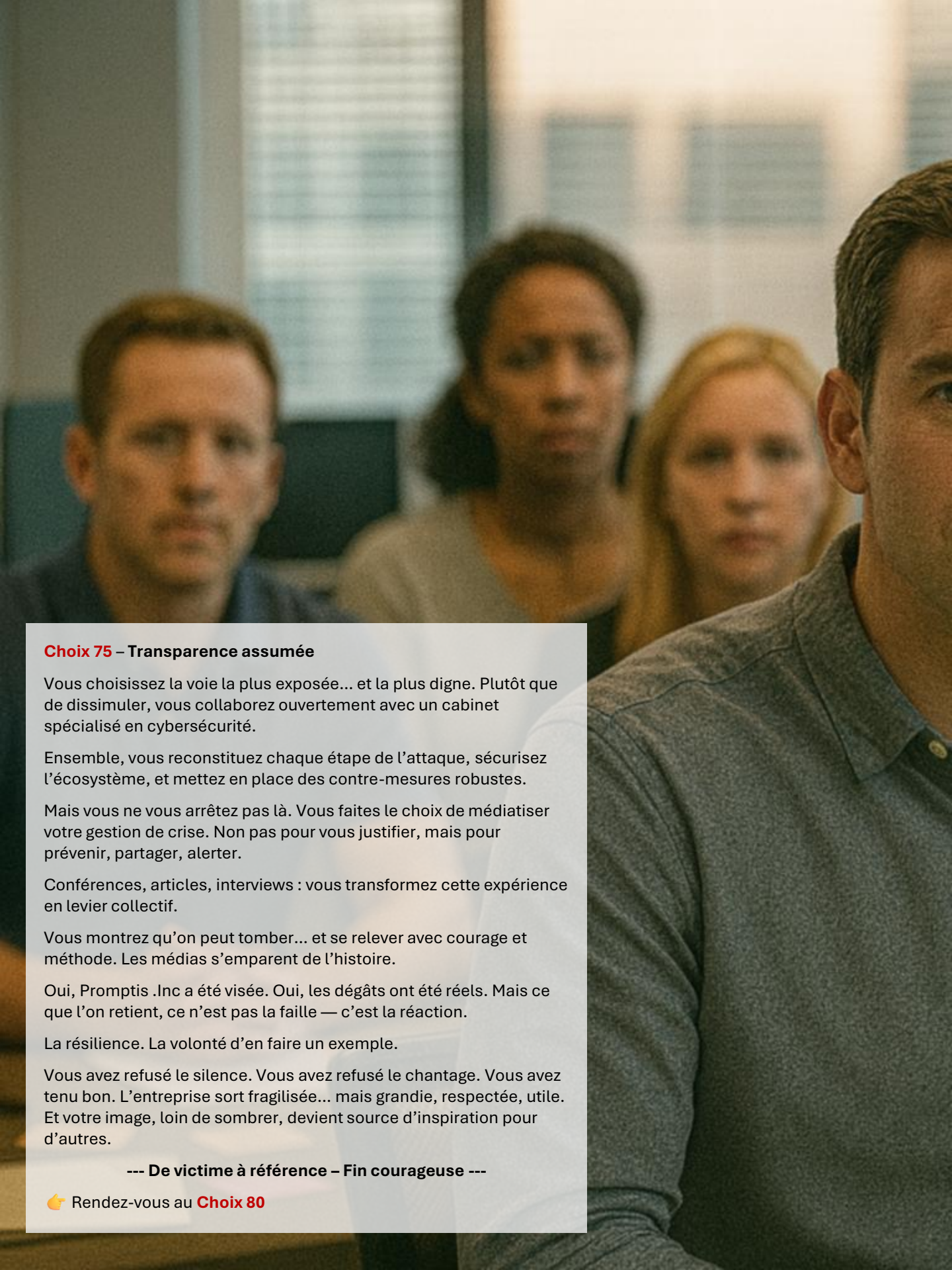
Le redémarrage est progressif, fragile, imparfait et prend plusieurs semaines — mais il tient. Et dans cette reconstruction prudente, un sentiment s'installe : celui d'avoir repris la main. Sans céder. Sans plier.

Chaque heure passée à rebâtir devient une leçon de rigueur. Chaque action documentée, un marqueur de résilience. Vous n'avez pas payé. Vous avez reconstruit.

Et surtout, en respectant la loi, vous avez envoyé un signal clair : ici, l'intégrité est non négociable.

--- Reconstruire sans plier - Fin honorable ---

👉 Rendez-vous au **Choix 80** pour le bilan.



Choix 75 – **Transparence assumée**

Vous choisissez la voie la plus exposée… et la plus digne. Plutôt que de dissimuler, vous collaborez ouvertement avec un cabinet spécialisé en cybersécurité.

Ensemble, vous reconstituez chaque étape de l'attaque, sécurisez l'écosystème, et mettez en place des contre-mesures robustes.

Mais vous ne vous arrêtez pas là. Vous faites le choix de médiatiser votre gestion de crise. Non pas pour vous justifier, mais pour prévenir, partager, alerter.

Conférences, articles, interviews : vous transformez cette expérience en levier collectif.

Vous montrez qu'on peut tomber… et se relever avec courage et méthode. Les médias s'emparent de l'histoire.

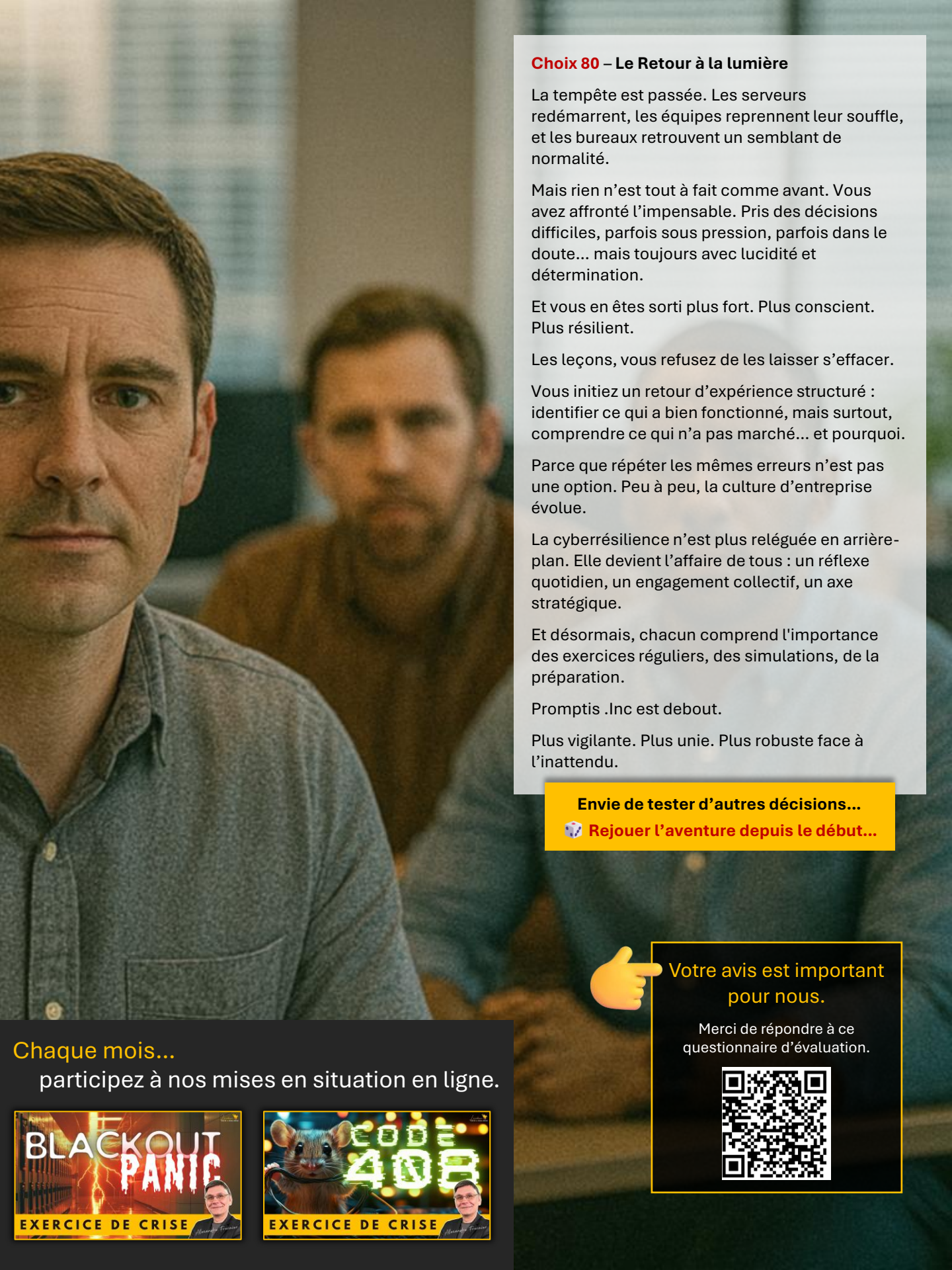
Oui, Promptis .Inc a été visée. Oui, les dégâts ont été réels. Mais ce que l'on retient, ce n'est pas la faille — c'est la réaction.

La résilience. La volonté d'en faire un exemple.

Vous avez refusé le silence. Vous avez refusé le chantage. Vous avez tenu bon. L'entreprise sort fragilisée… mais grandie, respectée, utile. Et votre image, loin de sombrer, devient source d'inspiration pour d'autres.

--- De victime à référence – Fin courageuse ---

👉 Rendez-vous au **Choix 80**



Choix 80 – Le Retour à la lumière

La tempête est passée. Les serveurs redémarrent, les équipes reprennent leur souffle, et les bureaux retrouvent un semblant de normalité.

Mais rien n'est tout à fait comme avant. Vous avez affronté l'impensable. Pris des décisions difficiles, parfois sous pression, parfois dans le doute… mais toujours avec lucidité et détermination.

Et vous en êtes sorti plus fort. Plus conscient. Plus résilient.

Les leçons, vous refusez de les laisser s'effacer.

Vous initiez un retour d'expérience structuré : identifier ce qui a bien fonctionné, mais surtout, comprendre ce qui n'a pas marché… et pourquoi.

Parce que répéter les mêmes erreurs n'est pas une option. Peu à peu, la culture d'entreprise évolue.

La cyberrésilience n'est plus reléguée en arrière-plan. Elle devient l'affaire de tous : un réflexe quotidien, un engagement collectif, un axe stratégique.

Et désormais, chacun comprend l'importance des exercices réguliers, des simulations, de la préparation.

Promptis .Inc est debout.

Plus vigilante. Plus unie. Plus robuste face à l'inattendu.

Envie de tester d'autres décisions…

🎲 **Rejouer l'aventure depuis le début…**

Votre avis est important pour nous.

Merci de répondre à ce questionnaire d'évaluation.

Chaque mois…

participez à nos mises en situation en ligne.

L'académie Crise & Résilience

L'unique Académie qui

Renforce votre Cyber Résilience,

une formation à la fois

FORMEZ-VOUS ICI

Code QR de l'académie

www.academiecriseetresilience.com

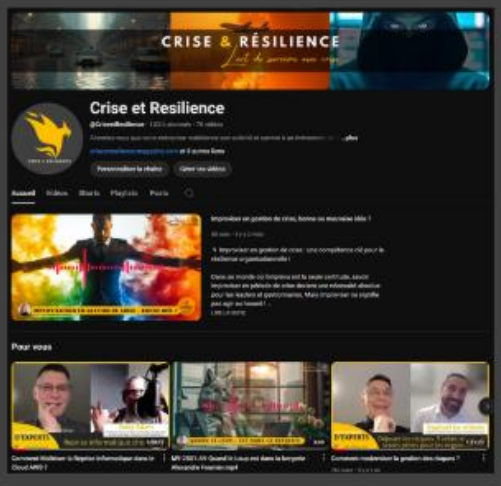
La chaîne youtube Crise & Résilience

L'unique chaîne Youtube qui

Renforce votre Cyber Résilience,

une vidéo à la fois

À REGARDEZ ICI



Code QR de Youtube

www.youtube.com/criseetresilience

Comment un cadre de gestion de crise peut être un outil précieux dans la lutte contre le terrorisme

Face à des menaces terroristes toujours plus imprévisibles et complexes, comment assurer une réponse efficace lorsque la prévention atteint ses limites ?

Cet article explore la puissance d'un cadre structuré de gestion de crise pour faire face à l'impossible : répondre de manière coordonnée, mesurable et humaine à l'horreur.

Lina Kolesnikova

Security and crisis management expert
Auteur du livre "Faire face aux prises d'otages massives. Cadre de gestion de crise"

Le terrorisme moderne ne se contente plus de faire des victimes ; il vise à paralyser les sociétés, à exploiter les vulnérabilités, et à défier les institutions.

Dans un monde où chaque territoire peut devenir une cible, il est devenu clair que la seule prévention ne suffit plus.

Face à cette réalité, une autre dimension de la lutte s'impose : celle de la gestion de la réponse. Car si l'on ne peut empêcher toutes les attaques, on peut en limiter les conséquences.

Et pour cela, il est essentiel de s'appuyer sur un cadre de gestion de crise structuré, anticipé et continuellement testé.

Ce document présente les grands principes d'une gestion efficace de la réponse aux attaques terroristes, en s'appuyant sur une approche systémique, des retours d'expérience et des recommandations concrètes.

Un nouveau visage du terrorisme : entre perception et impact réel

Avec les évolutions géopolitiques récentes, le terrorisme reste une menace bien présente.

Les actes d'intimidation, les attaques basées sur la perception, celles visant les services publics, les infrastructures critiques ou les civils ne semblent pas près de disparaître.

Le nombre d'attentats augmente. Les auteurs sont de plus en plus nombreux, mieux formés et mieux équipés.

En parallèle, nos sociétés restent vulnérables. Les forces de l'ordre, qu'elles soient internes ou externes, font face à de nombreuses limites : manque de personnel, de budget, de compétences et de capacités.

Notre capacité à répondre efficacement au terrorisme est mise à rude épreuve.

Pourquoi la gestion de la réponse est devenue cruciale

Il semble inévitable que des terroristes réussissent de temps à autre à perpétrer une attaque, qu'elle soit de petite ou de grande envergure.

Même si ce n'est pas le résultat souhaité, il est tout simplement impossible, ou du moins irréaliste, de protéger chaque personne et chaque endroit, à tout moment et en tout lieu.

La gestion des conséquences à court terme d'un événement et des conséquences à long terme des attaques est donc au premier plan de la lutte contre le terrorisme.

La réalité actuelle exige que tous les pays disposent d'instruments efficaces de gestion des crises antiterroristes, qu'ils les testent et les améliorent en permanence.

Les fondations d'une bonne gestion de crise

Contrairement aux activités de prévention et de dissuasion des attaques menées par des organismes hiérarchiques centralisés, la gestion de la réponse implique de multiples organisations issues de divers secteurs de la société.

Pour qu'une communauté soit réellement préparée, toutes les agences d'urgence doivent concevoir des plans compatibles entre eux, assurant une réponse cohérente.

Puisqu'il est impossible de garantir qu'aucune attaque ne surviendra, la manière dont nous réagissons devient essentielle.

La gestion de la réponse (pendant et après l'événement) influence fortement les conséquences d'une attaque terroriste.

Une réponse efficace permet de contenir les effets négatifs. À l'inverse, une mauvaise gestion peut amplifier les dégâts et entraîner des conséquences graves et durables.

Du concept à l'action : comment concevoir une réponse efficace

Que signifie une bonne gestion de la réponse ?

Elle intervient généralement après le début de l'attaque. Certaines situations, comme une prise d'otages, peuvent être de courte durée.

Mais dans la plupart des cas, la gestion de la réponse doit commencer pendant l'attaque et se poursuivre bien au-delà, pour traiter à la fois les conséquences immédiates et les effets à long terme.

La première caractéristique d'une bonne gestion de la réponse est donc qu'elle soit « *designed* » : pensée, structurée et préparée en amont pour fonctionner de manière efficace, pendant l'événement et dans la durée.

Le terme « *designed* » implique une conception anticipée : il ne s'agit pas d'improviser.

Les différents types d'attaques doivent être identifiés, et des critères d'efficacité doivent être définis.

Pour qu'un processus soit systématiquement efficace, il est essentiel de définir à l'avance les résultats attendus. Cela permet de guider sa conception en précisant :

- ce qu'il doit absolument accomplir (obligatoire et objectif),
- ce qui est souhaitable selon les conditions (recommandé ou conditionnel),
- ce qui est optionnel,
- et ce qui serait simplement « un plus » ou un avantage à intégrer si possible.

Tester, ajuster, répéter : une approche en amélioration continue

Une fois la conception terminée, la gestion de la réponse doit être mise en œuvre.

Mais cette mise en œuvre se heurte souvent à des limites : budgets réduits, ressources limitées. Il faut alors prendre des décisions pour trouver un équilibre.

Concrètement, cela signifie adapter les capacités nécessaires aux moyens disponibles. L'objectif est de maintenir l'efficacité tout en respectant les contraintes. C'est ce compromis qui permet de définir le faisable.

Autrement dit, ce que la gestion de la réponse peut réellement accomplir.

Il est aussi utile d'identifier ce qu'elle ne pourra pas accomplir, faute de moyens. Ces éléments deviennent alors des objectifs secondaires ou « agréables à avoir». Une fois ce faisable défini, le processus peut être testé et mesuré.

La gestion de la réponse doit pouvoir être activée à tout moment, sans préavis.

Cela suppose une disponibilité totale, 100 % du temps. Mais aussi une intégrité opérationnelle, pour garantir une réponse efficace à chaque activation.

Pour cela, l'état de préparation du processus doit être suivi en permanence. Il doit être régulièrement testé pour s'assurer qu'il fonctionne comme prévu.

Si les mesures ou les tests révèlent des failles, il faut corriger rapidement. Des ajustements doivent être faits. Et une fois ajusté, le processus doit de nouveau être mesuré, puis testé. Encore et encore.

C'est cette dynamique qui constitue la deuxième caractéristique clé d'une bonne gestion de la réponse :

Elle doit être anticipée, mise en œuvre, mesurée et continuellement améliorée.

Vers un cadre structuré : décomposer pour mieux agir

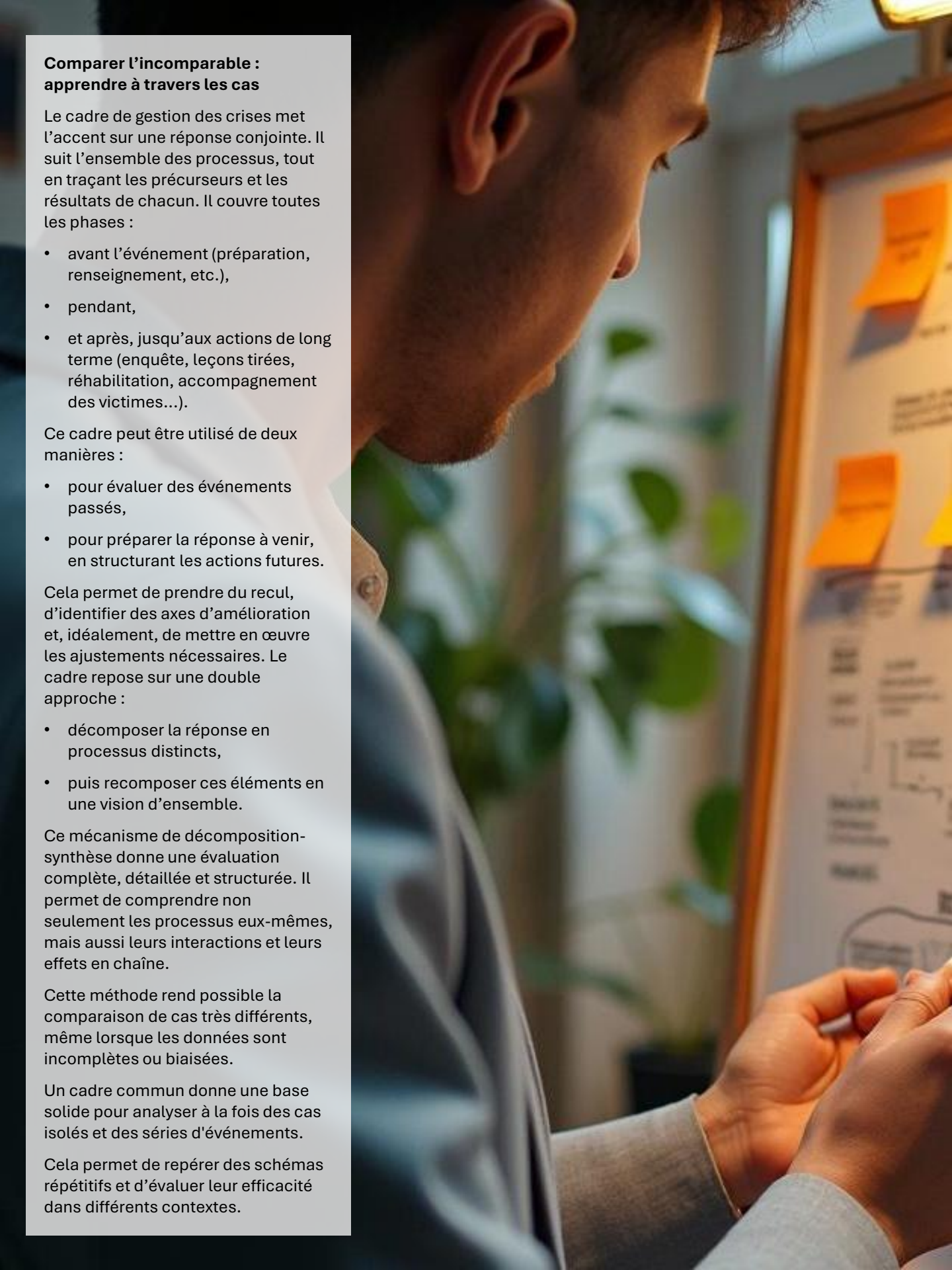
Comment procéder ?

Avec une telle diversité de types d'attaques, de géographies différentes et de toutes sortes d'organisations et d'entités impliquées, est-il possible de mettre en place une gestion de réponse complète ? Oui, nous le pouvons.

Nous pouvons utiliser une approche structurée, un cadre.

Les meilleurs cadres permettraient non seulement de mettre en place une gestion de réponse, mais aussi de la mesurer et de tirer des leçons structurées et cartographiables de l'analyse des situations précédentes.

Un tel cadre devrait couvrir la gestion de réponse dans son intégralité, y compris les activités qui ont lieu avant (état d'inactivité), pendant (à l'impact) et après l'attaque.



Comparer l'incomparable : apprendre à travers les cas

Le cadre de gestion des crises met l'accent sur une réponse conjointe. Il suit l'ensemble des processus, tout en traçant les précurseurs et les résultats de chacun. Il couvre toutes les phases :

- avant l'événement (préparation, renseignement, etc.),
- pendant,
- et après, jusqu'aux actions de long terme (enquête, leçons tirées, réhabilitation, accompagnement des victimes...).

Ce cadre peut être utilisé de deux manières :

- pour évaluer des événements passés,
- pour préparer la réponse à venir, en structurant les actions futures.

Cela permet de prendre du recul, d'identifier des axes d'amélioration et, idéalement, de mettre en œuvre les ajustements nécessaires. Le cadre repose sur une double approche :

- décomposer la réponse en processus distincts,
- puis recomposer ces éléments en une vision d'ensemble.

Ce mécanisme de décomposition-synthèse donne une évaluation complète, détaillée et structurée. Il permet de comprendre non seulement les processus eux-mêmes, mais aussi leurs interactions et leurs effets en chaîne.

Cette méthode rend possible la comparaison de cas très différents, même lorsque les données sont incomplètes ou biaisées.

Un cadre commun donne une base solide pour analyser à la fois des cas isolés et des séries d'événements.

Cela permet de repérer des schémas répétitifs et d'évaluer leur efficacité dans différents contextes.

Enfin, l'équipe examine l'ensemble des résultats produits :

- d'abord la décomposition,
- puis la synthèse,
- et enfin la comparaison de plusieurs cas avec le cadre comme référence.

Ce processus permet d'identifier clairement les lacunes, les faiblesses et les risques dans la gestion de la réponse, par exemple, dans un pays donné. Un tel niveau d'analyse renforce les recommandations et justifie la mise en œuvre d'améliorations concrètes.

Recommandations clés pour renforcer notre réponse collective

De nombreuses évaluations réalisées avec l'outil Cadre (Framework) de gestion de crise suggèrent que la gestion de la réponse aux attaques terroristes pourrait être améliorée en prenant en compte les suggestions suivantes – dont certaines sont difficiles à mettre en œuvre mais pourraient éclairer les développements législatifs futurs.

Au plus haut niveau :

- Planifier la réponse comme une mission de bout en bout – et non au niveau des agences individuelles, des catégories de victimes ou des processus. La planification de l'aide et de l'assistance aux victimes doit faire partie intégrante de toute réponse globale.
- Désigner une direction claire pour l'ensemble de l'opération – et pas seulement la responsabilité de certains aspects de celle-ci.
- Établir un centre d'information sous le contrôle des forces spéciales.
- Veiller à ce que les décisions professionnelles et techniques ne soient pas influencées par la politique – les responsables des services d'urgence peuvent alors accomplir leurs tâches sans pression politique.
- Établir et tester la liaison et la coopération entre les agences de manière à éviter toute confrontation institutionnelle ou personnelle, par exemple en créant un environnement non hostile dans lequel les services d'urgence peuvent travailler sans être soumis à des attitudes hostiles entre différentes organisations.

Au niveau des processus individuels, plusieurs suggestions générales peuvent être faites, notamment :

- Il faudrait introduire des cours de protection civile pour le public et la formation devrait être accessible et adaptable à tous, car nous sommes tous des victimes potentielles. Cela peut se faire par le biais de publicités sociales génériques, courtes et ciblées, ainsi que par le biais de programmes dédiés, chaque fois adaptés à des publics, des comportements ou des sujets sélectionnés.
- Un point de triage local, proche du site d'une attaque terroriste, devrait être envisagé (et planifié et formé) pour le traitement, le tri et l'expédition (le transport) des victimes chaque fois que la situation, ou sa détérioration éventuelle, pourrait laisser penser à un nombre important de victimes. L'expertise militaire en matière de formation et d'équipement des services d'urgence (par exemple pour la stabilisation et le traitement sur place) devrait être prise en compte, apprise et largement utilisée.
- Former les personnes chargées d'aider les victimes d'actes terroristes. Il est nécessaire de créer un centre de services pour la psychologie des catastrophes, où la prise en charge des victimes d'attentats terroristes en ferait partie.
- Apprendre la mentalité, le passé et les circonstances des terroristes et, surtout, de ceux qui peuvent être impliqués dans le terrorisme contre leur gré, par la force ou en raison des circonstances, des préjugés culturels, sociaux ou ethniques.
- Créer un fonds spécifique pour indemniser les victimes du terrorisme pour les dépenses personnelles liées au terrorisme, y compris les services médicaux et de santé mentale, la perte de salaire, les frais d'inhumation, l'assistance juridique et la défense des droits.

Tirer les leçons, agir avant d'être frappés

Les conséquences émotionnelles du terrorisme posent de grands défis aux responsables de la planification de la prévention et de la réponse.

Cela soulève d'importantes questions sur la capacité d'un système de santé publique à comprendre et à se préparer à de tels événements.

Il est important de tirer les leçons de l'expérience d'autres pays afin de minimiser l'impact d'éventuelles attaques terroristes dans votre propre pays.

Des dispositions spécifiques devraient être mises en œuvre pour garantir que les leçons sont tirées et que toutes les activités, y compris le soutien et l'assistance aux victimes, sont adaptées aux exigences d'une nouvelle réalité après les attaques terroristes.

Tirez les leçons des États qui ont déjà connu des attaques de grande ampleur, n'attendez pas une telle expérience sur votre propre sol.

Dans un monde où l'imprévisible devient la norme, la réactivité ne peut plus être improvisée.

La gestion de la réponse aux attaques terroristes doit être conçue comme un processus structuré, transversal et dynamique, capable de s'adapter, de s'améliorer et de protéger ce qui peut l'être.

Un cadre rigoureux permet de transformer le chaos en action coordonnée, d'identifier les failles pour mieux les combler, et de replacer les victimes au cœur de l'intervention.

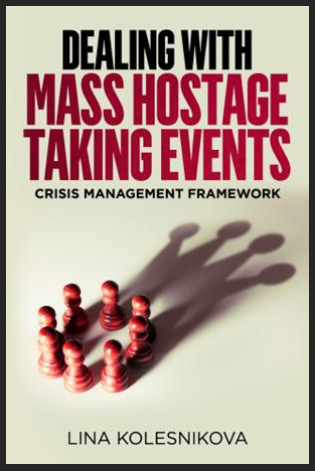
Plus qu'un outil technique, c'est un levier de résilience pour les sociétés modernes.

Préparer l'après, c'est déjà lutter contre le terrorisme.

Lina Kolesnikova

Auteur du livre *"Dealing with Mass Hostage Taking Events – Crisis Management Framework"*, expert international en gestion de crise, sécurité urbaine et contre-terrorisme, intervenant pour l'UNOCT, l'OSCE et l'EFUS.
Coordinateur de projets européens (Horizon2020, ISF), conférencier reconnu (Milipol, UNOCT, World Police Summit…) et contributeur régulier à de nombreuses publications spécialisées.
Influenceur du secteur sécurité (Global Influencers List 2023/2024), multilingue et auteur de scénarios pour red teams.

À LIRE *DU MÊME AUTEUR …*



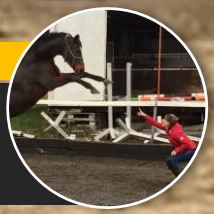
Le cheval, un partenaire unique en gestion de crise

Découvrez comment le cheval, partenaire inédit en gestion de crise, développe un leadership authentique, agile et fédérateur.

Apprenez à transformer vos équipes grâce à la puissance naturelle des chevaux, révélant ainsi une cohésion exceptionnelle, la « pensée unique », essentielle pour traverser efficacement toute situation complexe et incertaine.

Pierre Aubry et Magali Marti

Pierre. Expert en gestion de crise
Analyse de risques, gestion de crise, gestion de projet en lien avec la sécurité
Magali. Experte en leadership avec le cheval
Accompagnement individuel et de groupe avec les chevaux



Dans un monde marqué par l'incertitude, les crises exigent des réponses transparentes, rapides, coordonnées et efficaces.

Au cœur de ces réponses se trouve un leadership authentique et agile, capable de rassembler et mobiliser les équipes vers une vision commune.

Or, le cheval se révèle être un partenaire exceptionnel pour développer ce type de leadership.

La puissance du leadership inspiré par les chevaux

Le cheval, en tant qu'animal proie, possède des compétences innées de gestion de crise : organisation collective, rapidité de réaction et résilience face au danger.

Lorsqu'un troupeau décide de se déplacer pour fuir un prédateur, tous les individus partent simultanément, à la même vitesse et dans la même direction, illustrant parfaitement l'objectif de tout groupe humain confronté à une crise.

CRÉDIT PHOTO : Pierre Aubry et Magali Marti

C’est précisément ce phénomène que nous observons et que nous transposons dans le contexte de l'entreprise ou de toute organisation.

En travaillant avec les chevaux, les leaders apprennent à se synchroniser naturellement avec leur équipe.

Cette expérience permet de révéler les dynamiques authentiques de groupe favorisant l’émergence d’une « pensée unique ».

Cette dernière est une forme supérieure de cohésion où chaque membre, indépendamment de son rôle hiérarchique, contribue pleinement à la puissance collective en abandonnant momentanément sa position pour la réussite du groupe.

Ce processus d’apprentissage par l’expérience directe encourage aussi les individus à mieux comprendre les notions d'empathie, d’écoute active et de reconnaissance mutuelle, des qualités essentielles pour gérer efficacement les crises au sein des organisations.

Du faire-faire au savoir-faire : une transition essentielle

En cas de crise, à savoir de besoin de fuite, le cheval refuse instinctivement le rapport dominant/dominé fondé sur la contrainte.

En accompagnement avec le cheval, les **managers dominants** qui cherchent à imposer leur volonté par la force ou l'autorité découvrent rapidement leurs limites.

En revanche, un **leader véritable** facilite une transition cruciale : celle du faire-faire au savoir-faire.

Cette transition, expérimentée concrètement lors des séances d’accompagnement avec les chevaux, renforce la responsabilisation des collaborateurs et libère les potentiels individuels contribuant ainsi à une performance collective accrue.

Au-delà de cette transition essentielle, le travail avec les chevaux met également en évidence l'importance d'une communication claire et ouverte au sein des équipes.

Les managers découvrent comment transmettre une vision commune tout en laissant à chacun l'espace nécessaire pour exprimer ses talents spécifiques et contribuer efficacement au succès global du projet ou de la gestion d'une crise.

Identifier et lever les blocages grâce au cheval

En situation de crise ou de changement profond (fusion, réorganisation, évolution managériale), les résistances internes sont fréquentes.

L'interaction avec le cheval met rapidement en lumière ces blocages permettant au leader de les identifier et de les résoudre efficacement.

Le cheval agit comme un miroir transparent des dynamiques interpersonnelles et organisationnelles, révélant les résistances et encourageant naturellement un leadership fédérateur plutôt qu'autoritaire.

De plus, les exercices avec les chevaux offrent l'opportunité de tester différentes stratégies de communication et de résolution des conflits en temps réel.

Cette expérimentation concrète permet de mieux comprendre les mécanismes sous-jacents aux résistances tout en fournissant des outils pratiques pour désamorcer les tensions et construire une collaboration durable au sein des équipes.

Leadership naturel vs domination

Il est fondamental de distinguer clairement le leadership naturel de la simple domination.

Tandis que le dominant utilise souvent la peur ou l'autorité pour parvenir à ses fins, le leader naturel inspire, rassure, rassemble et motive par son exemplarité et son intégrité.

Le cheval nous enseigne que la véritable puissance réside dans la capacité à fédérer pacifiquement et efficacement un groupe, non dans l'exercice autoritaire d'un pouvoir personnel.

CRÉDIT PHOTO : Pierre Aubry et Magali Marti

Cette distinction est particulièrement cruciale dans les environnements où la pression est élevée et où les comportements dominants peuvent rapidement devenir toxiques.

Le cheval offre alors un cadre sûr et efficace pour remettre en question ces comportements et encourager l'adoption d'un leadership plus éthique et respectueux des valeurs humaines.

Le cheval, source intarissable d'inspiration

En conclusion, travailler avec le cheval en gestion de crise et leadership est bien plus qu'une méthode éprouvée. C'est une philosophie pratique qui allie intuition, observation et action.

À travers les enseignements naturels du cheval, guidés par un professionnel, les dirigeants découvrent comment mobiliser authentiquement leur équipe autour d'un projet commun, renforçant ainsi la résilience, l'agilité et la crédibilité organisationnelle nécessaires à la réussite en situation complexe.

Le cheval devient ainsi un partenaire précieux non seulement pour gérer les crises, mais aussi pour anticiper et se préparer efficacement aux défis futurs.

Pierre Aubry et Magali Marti

Expérience vécue

Témoignage de Pierre Aubry

Lorsque je suis arrivé sur le carré de sable accompagné de Dezcalia, la jument de Magali, ma première approche était douce, respectueuse et progressive.

Je souhaitais établir un premier contact calme, sans brusquerie pour créer une connexion basée sur la confiance. Après quelques instants, j'ai pu lui caresser l'épaule tout en lui adressant un bonjour chaleureux. Dezcalia me regardait attentivement comme si elle attendait davantage de ma part.

En fixant ses oreilles, j'ai tenté de lui expliquer calmement que je voulais l'inviter à marcher ensemble autour du carré. En initiant la marche devant elle, je remarquai rapidement qu'elle restait immobile, observatrice, mais passive, puis, finalement elle décida de s'éloigner pour brouter tranquillement sur les bordures, manifestant clairement son désintérêt.

Perplexe, je me suis questionné sur ce qui avait pu provoquer cette réaction.

À ce moment, Magali est intervenue avec justesse en me demandant de m'interroger sur mon niveau réel de détermination par rapport à mon objectif.

Elle m'a rappelé l'importance d'exprimer clairement et fermement mes intentions afin que Dezcalia puisse ressentir une confiance suffisante pour me suivre spontanément.

Fort de ce conseil précieux, j'ai recentré mon attention sur mon intention profonde et mon objectif précis.

En visualisant mentalement le chemin à suivre, je me suis de nouveau approché de Dezcalia avec détermination.

D'un ton à la fois rassurant et affirmé, je lui ai clairement communiqué mon intention tout en accompagnant mes paroles d'un geste corporel franc et précis indiquant la direction souhaitée. Immédiatement, Dezcalia s'est mise en mouvement et m'a suivi sans hésitation.

Cette expérience m'a enseigné de manière très concrète à mieux clarifier mes intentions et à les transmettre avec confiance et détermination tant sur le plan verbal que corporel.

Grâce à cette prise de conscience, j'ai pu maintenir une approche douce et respectueuse tout en affirmant pleinement mon leadership naturel.

L'académie Crise & Résilience

L'unique Académie qui

Renforce votre Cyber Résilience,

une formation à la fois

FORMEZ-VOUS ICI

Code QR de l'académie

www.academiecriseetresilience.com

Gestion de crise : pourquoi la séquence pédagogique change tout[(1)]

La clé d'une formation réussie en gestion de crise réside moins dans les méthodes utilisées que dans leur ordre d'utilisation.

Découvrez comment une séquence pédagogique optimale, intégrant simulations et théorie, permet d'acquérir une expertise véritablement adaptée aux crises d'aujourd'hui, bien au-delà des approches traditionnelles.

La source : (1) De Vittoris, R., & Cros, S. (2022). Crisis management learning: when the sequence of pedagogic levers counts more than the levers themselves. Vie & sciences de l'entreprise, 214-215(2), 167-194.

https://shs.cairn.info/revue-vie-et-sciences-de-l-entreprise-2022-2-page-167?lang=en

Raphaël de Vittoris

Symbio Director Risk Management / Internal Control / Progress / Cyber / Security – Associate Professor Strategy & Crisis Mgt – Founder Antifragile.fr

Face à des crises imprévisibles et complexes, préparer efficacement les décideurs devient crucial.

Une étude novatrice démontre que l'efficacité des formations en gestion de crise dépend davantage de la séquence pédagogique mise en œuvre que des méthodes employées individuellement.

Cette découverte change profondément notre vision de l'apprentissage en crise.

Longtemps, les formations à la gestion de crise ont accumulé méthodes et outils pédagogiques variés (simulations, serious games, cours théoriques) sans réfléchir à leur ordre précis.

Pourtant, une recherche récente révèle que c'est la « séquence » de ces outils qui conditionne la profondeur réelle de l'apprentissage.

> Cette étude introduit le concept de « sédimentation cognitive » : chaque étape pédagogique laisse une empreinte cognitive qui s'accumule et structure progressivement une expertise solide.

Ainsi, une même combinaison d'outils produit des résultats radicalement différents selon l'ordre dans lequel ils sont déployés.

Une simulation de crise suivie d'une réflexion théorique génère une compréhension beaucoup plus riche qu'un ordre inverse (théorie puis simulation) qui se révèle le pire schéma pédagogique alors qu'il est justement majoritairement déployé par les entreprises.

Pour mesurer précisément ces effets, l'étude utilise des « cartes cognitives », un outil de représentation mentale développé par Novak (1977)[(2)], permettant de visualiser concrètement la manière dont l'apprenant organise ses connaissances.

Avant et après chaque session, les participants dessinent leur compréhension des crises.

Résultat : une séquence optimale (simulation → théorie) produit des cartes très riches en concepts et en connexions, traduisant un apprentissage profond et structuré. À l'inverse, une séquence moins efficace laisse une carte cognitive appauvrie.

(2) *Novak, J. D. (1977). An alternative to piagetian psychology for science and mathematics education. Science Education, 61(4), p. 453–477. https://doi.org.10.1002/sce.3730610403*

Les serious games occupent une place centrale dans cette pédagogie innovante.

Ces jeux immersifs permettent une pratique sécurisée et réaliste des décisions en crise, stimulant un engagement actif crucial pour la mémorisation à long terme (Cros & Vraie, 2018)[3].

Une séquence incluant d'abord une préparation théorique en vidéo suivie d'un serious game offre des résultats significativement meilleurs qu'une approche inversée, confirmant ainsi la nécessité d'un ordre progressif de passif à interactif.

Le résultat ultime de ces séquences pédagogiques optimisées est une « complexification cognitive ».

Les décideurs développent une représentation mentale plus riche, nuancée et flexible, les rendant capables d'adaptation face à l'inédit.

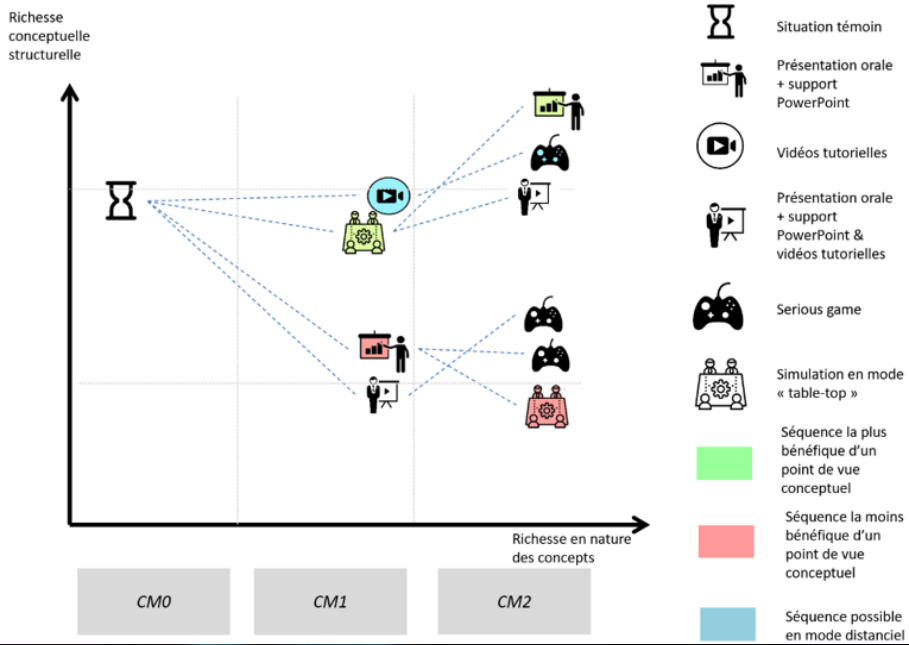
Ce modèle fait écho à l'apprentissage expérientiel théorisé par Kolb (2014)[4] :

alterner expérience concrète et réflexion théorique maximise l'acquisition et la structuration des connaissances.

Ainsi, former efficacement à la gestion de crise implique de repenser radicalement les parcours pédagogiques traditionnels pour intégrer des séquences d'apprentissage structurées où simulations, jeux sérieux et réflexions théoriques se succèdent selon un ordre précis.

Cette approche crée une résilience réelle en permettant aux décideurs de mobiliser rapidement des connaissances complexes et adaptatives en situation de crise.

(3) Cros, S., Vraie, B. (2018). De l'intérêt des serious games comme méthode de restitution des apprentissages, sous stress aigu, en crise. Management et Avenir, 102(4), p. –66. https://doi.org.10.3917/mav.102.0051
(4) Kolb, D. A. (2014). Experiential learning: Experience as the source of learning and development. FT press.



Les lettres CM signifient « cartographie cognitive » (=Cognitive Maps). Il y en a 3 car j'ai procédé à 3 cartographies successives intercalée par les actions pédagogiques.

En somme, l'expérience débutait avec une cartographie cognitive originelle (CM0). Celle-ci était suivie d'une action par un levier pédagogique. Une fois cette action effectuée, nous passions à une nouvelle cartographie cognitive (CM1) afin d'évaluer comment la conception de la crise avait évoluée dans l'esprit des sujets.

Nous passions alors à l'utilisation d'un 2e levier pédagogique. Il était suivi d'une nouvelle cartographie cognitive (CM2).

Pour résumer : c'est l'analyse de l'évolution de ces cartographies cognitives successives (qui s'intercalaient entre les différents leviers pédagogiques utilisé dans toutes les combinaisons possibles) qui m'a permis d'identifier la séquence pédagogique la plus pertinente pour développer une pensée complexe et une mémorisation accrue des principes de gestion de crise.

Conclusion

Cette étude révolutionnaire invite les organisations à dépasser les approches pédagogiques classiques en gestion de crise.

Loin d'une simple accumulation d'outils, c'est la qualité de leur enchaînement qui garantit une expertise profonde et adaptative.

Les responsables doivent désormais concevoir leurs parcours de formation en intégrant simulations, jeux sérieux et enseignements théoriques dans une logique cohérente et progressive.

Ce nouveau paradigme pédagogique offre un avantage décisif en matière de résilience, préparant les décideurs à naviguer efficacement dans la complexité croissante des crises contemporaines.

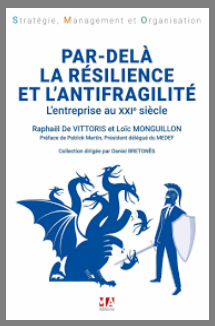
Raphaël de Vittoris

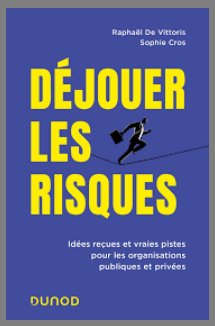
Raphaël De Vittoris est directeur des risques, de la crise et de la cyberdéfense chez Symbio. Docteur en sciences de gestion, il est aussi professeur associé et fondateur d'Antifragile.fr.Auteur de plusieurs ouvrages, il explore la résilience et l'antifragilité des organisations. Il accompagne les entreprises dans la consolidation de leur pérennité.Son parcours mêle recherche, enseignement et action, au croisement du management, de la stratégie et de la gestion de crise.

https://antifragile.fr/

À LIRE

DU MÊME AUTEUR ...





Abonnez-vous pour recevoir les prochains articles scientifiques de Raphaël de Vittoris.

www.magazinecriseetresilience.com

Mise en pratique

Pour intégrer efficacement cette approche innovante dans vos formations, que vous soyez une grande entreprise ou une PME, suivez ces étapes concrètes :

1. **Diagnostic initial personnalisé :** Identifiez d'abord clairement le niveau initial de préparation de vos équipes via questionnaires ou entretiens, complétés idéalement par une première carte cognitive individuelle décrivant leur vision actuelle de la gestion de crise. Cela vous permet de repérer précisément les lacunes à combler.
2. **Construire une séquence pédagogique optimale :** Commencez systématiquement par une simulation de crise (tabletop, jeu de rôle) qui expose immédiatement vos participants aux réalités complexes et imprévisibles. Cette immersion initiale crée un besoin réel d'apprendre.
3. **Apports théoriques ciblés et pertinents :** Suivez par une session structurée qui apporte des concepts théoriques essentiels (en présentiel ou via e-learning). Le contenu doit éclairer directement les défis expérimentés lors de la simulation initiale.
4. **Intégration des serious games :** Utilisez ensuite un serious game, numérique ou présentiel, permettant aux apprenants de tester ces nouveaux savoirs dans un environnement ludique et sécurisé. Cela favorise une mémorisation active et durable.
5. **Session finale de débriefing réflexif :** Concluez par une discussion collective approfondie analysant l'ensemble des expériences vécues et concepts théoriques abordés. Les échanges permettent de cristalliser les apprentissages et de renforcer les compétences collectives.
6. **Mix digital et présentiel équilibré :** Pour les grandes entreprises, privilégiez des plateformes immersives complexes, tandis que les PME peuvent adopter des formats plus légers comme des ateliers ou des modules e-learning combinés à des simulations simples.

En adoptant cette approche séquentielle cohérente, vous maximiserez l'efficacité de vos formations à la gestion de crise, développant ainsi une résilience organisationnelle robuste face aux défis actuels et futurs.

L'académie Crise & Résilience

L'unique Académie qui

Renforce votre Cyber Résilience,

une formation à la fois

FORMEZ-VOUS ICI

Code QR de l'académie

www.academiecriseetresilience.com

Et si la cybersécurité était un levier de croissance?

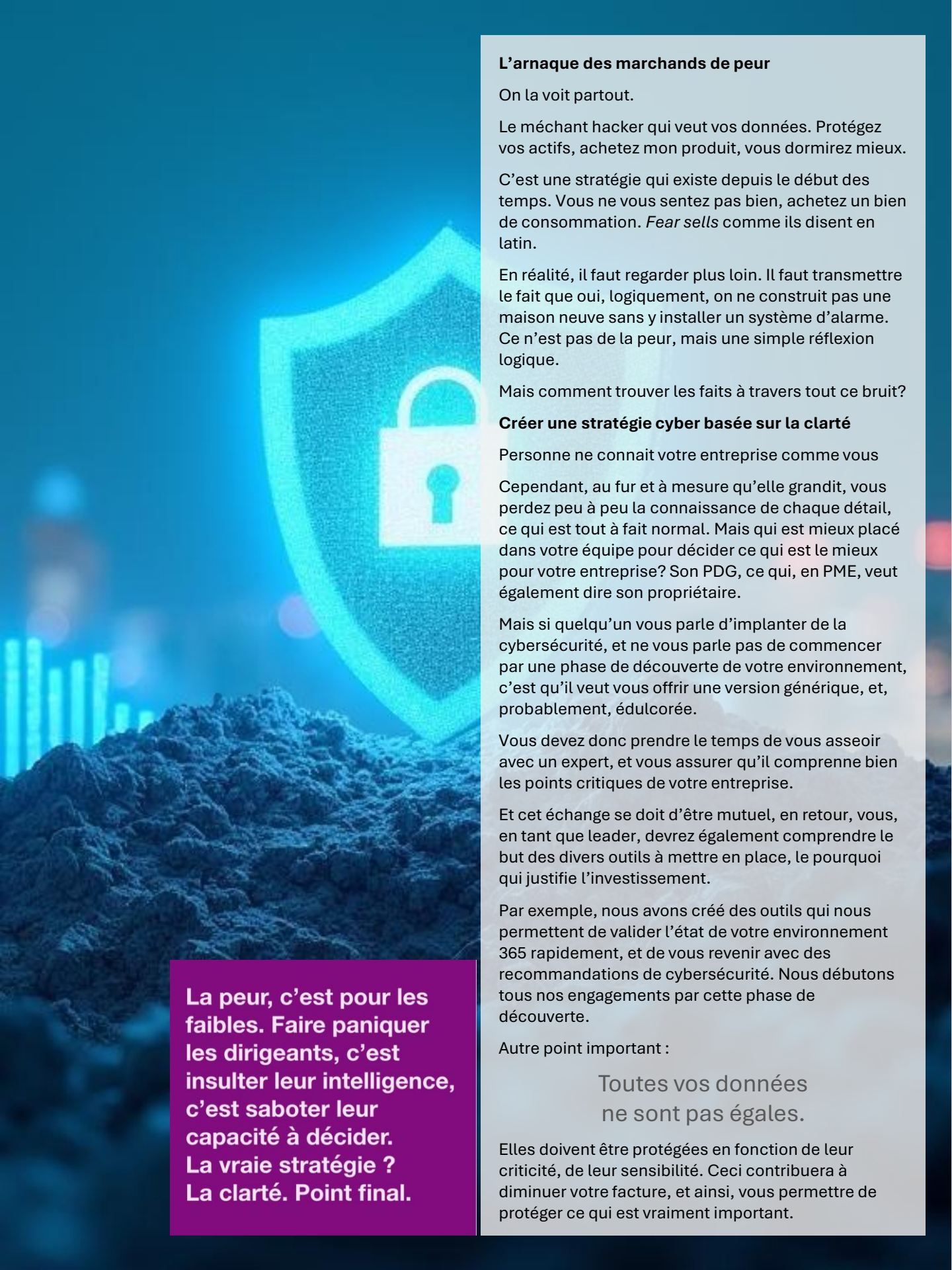
On parle toujours de cybersécurité comme d'une dépense, d'un centre de coûts, ou encore pire : un risque.

Et si, en vérité, la cybersécurité était le levier dont votre petite et moyenne entreprise (PME) a besoin pour accélérer sa croissance?

Matière à réflexion pour PDG allumé.

René-Sylvain Bédard

René-Sylvain est un expert Microsoft, un entrepreneur, un mentor et un conférencier dans le domaine de l'infrastructure informatique et de la cybersécurité.



La peur, c'est pour les faibles. Faire paniquer les dirigeants, c'est insulter leur intelligence, c'est saboter leur capacité à décider. La vraie stratégie ? La clarté. Point final.

L'arnaque des marchands de peur

On la voit partout.

Le méchant hacker qui veut vos données. Protégez vos actifs, achetez mon produit, vous dormirez mieux.

C'est une stratégie qui existe depuis le début des temps. Vous ne vous sentez pas bien, achetez un bien de consommation. *Fear sells* comme ils disent en latin.

En réalité, il faut regarder plus loin. Il faut transmettre le fait que oui, logiquement, on ne construit pas une maison neuve sans y installer un système d'alarme. Ce n'est pas de la peur, mais une simple réflexion logique.

Mais comment trouver les faits à travers tout ce bruit?

Créer une stratégie cyber basée sur la clarté

Personne ne connait votre entreprise comme vous

Cependant, au fur et à mesure qu'elle grandit, vous perdez peu à peu la connaissance de chaque détail, ce qui est tout à fait normal. Mais qui est mieux placé dans votre équipe pour décider ce qui est le mieux pour votre entreprise? Son PDG, ce qui, en PME, veut également dire son propriétaire.

Mais si quelqu'un vous parle d'implanter de la cybersécurité, et ne vous parle pas de commencer par une phase de découverte de votre environnement, c'est qu'il veut vous offrir une version générique, et, probablement, édulcorée.

Vous devez donc prendre le temps de vous asseoir avec un expert, et vous assurer qu'il comprenne bien les points critiques de votre entreprise.

Et cet échange se doit d'être mutuel, en retour, vous, en tant que leader, devrez également comprendre le but des divers outils à mettre en place, le pourquoi qui justifie l'investissement.

Par exemple, nous avons créé des outils qui nous permettent de valider l'état de votre environnement 365 rapidement, et de vous revenir avec des recommandations de cybersécurité. Nous débutons tous nos engagements par cette phase de découverte.

Autre point important :

Toutes vos données
ne sont pas égales.

Elles doivent être protégées en fonction de leur criticité, de leur sensibilité. Ceci contribuera à diminuer votre facture, et ainsi, vous permettre de protéger ce qui est vraiment important.

L'importance de protéger sa réputation

Si, comme moi, vous êtes un propriétaire d'entreprise, vous connaissez la valeur de la réputation de votre entreprise. Certains vont jusqu'à calculer le nombre de clients qui sont attirés et retenus grâce à la force de la marque.

Donc, de ce point de vue, la cybersécurité devient un actif, dont le but est de protéger votre marque.

Si, par exemple, vous publiiez sur vos réseaux sociaux le nombre d'attaques repoussées ce mois-ci. Est-ce que vous croyez que ceci aurait un effet négatif ou positif sur votre réputation?

La cybersécurité pour sécuriser de nouveaux clients

Vous souhaitez prendre de l'expansion, conquérir de nouveaux clients, voir même, doubler votre chiffre d'affaires de l'an dernier?

Vous aurez besoin de la cybersécurité pour y arriver. Pourquoi?

Parce que, sans ce niveau de sécurité et de validation, vos plus grands clients refuseront probablement de faire affaire avec vous. Les grands comptes demandent désormais des preuves que votre entreprise est SÉCURE. Ceci prend souvent la forme de sondage, avant la signature du contrat, est-ce que vous avez tel type d'outil, est-ce que vous avez un centre de surveillance, quand était votre dernier test d'intrusion, pouvons-nous voir le rapport, et quels ont été les correctifs mis en place.

Ou encore mieux : Détenez-vous la certification ISO 27001, ou SOC 2?

Ces dernières arrivent avec des critères de sécurité encore plus stricte.

Donc, vous souhaitez signer ce nouveau client à 1,000,000$? Investissez en cybersécurité.

Investir en cybersécurité, d'accord, mais à quel prix?

En tant qu'entrepreneurs, nous connaissons tous le concept du coût d'opportunité.

Je vous entends déjà poser la question, « Est-ce que cela va me couter un million pour obtenir ce contrat? », la réponse courte : non, cela n'a pas besoin d'être aussi dispendieux pour être efficace.

Vous vous souvenez, en début d'article, j'expliquais que vous deviez maitriser vos données et vos services critiques?

C'est la manière de faire pour mettre en place une stratégie de cybersécurité efficace, en maintenant des coûts raisonnables.

Par exemple, protéger vos appareils, chez Indominus Sécurité Gérée, débute à 9.99 par appareils par mois. C'est moins dispendieux qu'un service cellulaire. Donc, sur cette base, quelle bonne raison auriez-vous pour vous priver d'un service de télésurveillance 24/7? Encore une fois, exactement le même principe que pour votre résidence, une centrale d'alarme, qui surveille en temps réel.

Prenez le temps d'y mettre l'attention nécessaire, faites-en une priorité, et vous réaliserez assez rapidement que des solutions existent, et qu'elles ne sont pas toutes exorbitantes.

Conclusion

Depuis trop longtemps, les manufacturiers et certains marchands de peur vous démontrent que la cybersécurité est un bouclier. J'en ai également été coupable dans certains de mes raisonnements antérieurs. En revanche, nous pouvons désormais voir les preuves.

La cybersécurité est un investissement, un levier de croissance. Et se faisant, il faut s'en servir pour avancer, pour sécuriser de nouveaux clients et croitre.

Je vous souhaite donc un futur rempli de défi et de croissance, supporté par la cybersécurité.

René-Sylvain Bédard

Depuis plus de 30 ans, j'aide les PME à transformer la cybersécurité en moteur de croissance, et pas en dépense ou en contrainte.

En tant que Partenaire Microsoft certifié et fondateur d'Indominus, j'ai conçu des outils pour démocratiser la cybersécurité et permettre aux propriétaires d'entreprises de se les approprier.

Je suis également auteur et conférencier, mon livre Conçu pour être SÉCURE, est un guide pour leader souhaitant intégrer la cybersécurité dans la culture de son entreprise, et ainsi, lui permettre de croître.

EN BONI : Si vous souhaitez discuter de cybersécurité, je vous offre un entretien gratuit de 25 minutes. Réservez-la ici: https://bit.ly/In-25minutes.

Indominus
Sécurité Gérée

https://indominus.ms/fr/

L’anticipation, levier stratégique pour piloter dans la complexité

Anticiper, c’est maîtriser notre savoir organisationnel pour ne rien laisser au hasard : acteurs clés, planification, retours d’expériences.

Fonction stratégique, l’anticipation repose sur une méthodologie et des agents préparés régulièrement.

L’essentiel : une écoute active de la cellule décisionnelle pour éclairer et accompagner le décideur dans ses choix.

Tanguy BORNET

Responsable du maintien en condition opérationnelle
Expertise en gestion de crise et sécurité globale appliquée
Direction générale de la santé centre de crises sanitaires

Anticiper, c’est structurer l’action face à l’incertain. En s’appuyant sur notre savoir organisationnel, nous préparons les décisions d’aujourd’hui pour rendre possibles les manœuvres de demain.

Dans une société des organisations toujours plus interdépendante, l’anticipation devient une fonction stratégique essentielle pour guider l’action sans s’y substituer.

Anticiper, c’est structurer notre intelligence collective

Anticiper ne consiste pas à prévoir l’avenir, mais à créer les conditions d’une réponse organisée et crédible à des événements incertains. Cela commence par un travail sur le savoir organisationnel : savoir qui fait quoi, avec qui, selon quelles modalités. Cette étape permet d’éviter un risque majeur en contexte incertain : l’improvisation désordonnée.

Identifier les bons acteurs, cartographier les partenaires, planifier les séquences d’action possibles, et capitaliser les retours d’expérience vécus ou observés sont autant de gestes fondateurs. Ce socle garantit une capacité d’action coordonnée, réactive et pertinente, même sous pression.

Dans cette logique, la planification n’est pas un carcan : elle est un support de manœuvre. Elle prépare, sans prédéterminer. Elle permet de penser l’exception dans la norme, de rendre l’improbable pensable sans prétendre le domestiquer.

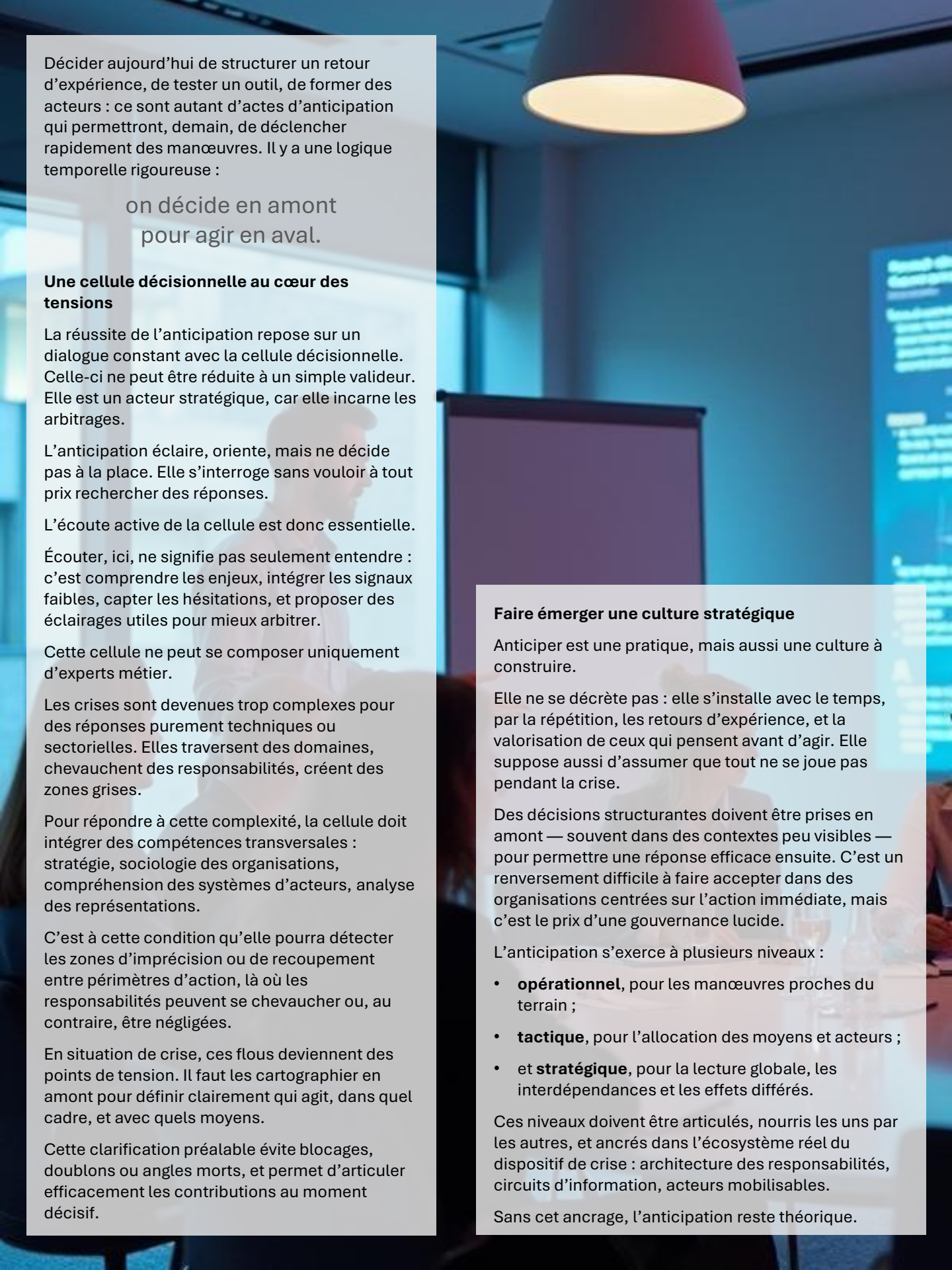
Construire une fonction stratégique face au brouillard

Toute démarche d’anticipation sérieuse passe ensuite par une analyse de risque. Ce travail consiste à construire des scénarios minorants, médiants ou majorants[1], pour calibrer l’action future. Ces scénarios ne cherchent pas à prédire, mais à exercer l’organisation à penser l’incertain, dans toute sa profondeur et sa volatilité.

Cette approche s’inscrit dans les principes fondamentaux de la stratégie : le brouillard stratégique — cette opacité inhérente aux situations complexes — ne se dissipe jamais totalement.

Mais l’anticipation, en tant que fonction stratégique, vise à le réduire, en dégageant lignes de force, points d’appui, vulnérabilités.

(1) Le **scénario minorant** correspond à une hypothèse de crise dans laquelle les impacts sont supposés être les plus faibles possibles, tout en restant plausibles. Le **scénario médian** représente une situation de crise d’intensité moyenne, considérée comme la plus probable. Il est souvent utilisé comme base de planification opérationnelle. Le **scénario majorant** envisage une situation extrême, avec des conséquences maximales. Il permet de tester les limites du système de gestion de crise et d’identifier les points de rupture potentiels.



Décider aujourd'hui de structurer un retour d'expérience, de tester un outil, de former des acteurs : ce sont autant d'actes d'anticipation qui permettront, demain, de déclencher rapidement des manœuvres. Il y a une logique temporelle rigoureuse :

on décide en amont
pour agir en aval.

Une cellule décisionnelle au cœur des tensions

La réussite de l'anticipation repose sur un dialogue constant avec la cellule décisionnelle. Celle-ci ne peut être réduite à un simple valideur. Elle est un acteur stratégique, car elle incarne les arbitrages.

L'anticipation éclaire, oriente, mais ne décide pas à la place. Elle s'interroge sans vouloir à tout prix rechercher des réponses.

L'écoute active de la cellule est donc essentielle.

Écouter, ici, ne signifie pas seulement entendre : c'est comprendre les enjeux, intégrer les signaux faibles, capter les hésitations, et proposer des éclairages utiles pour mieux arbitrer.

Cette cellule ne peut se composer uniquement d'experts métier.

Les crises sont devenues trop complexes pour des réponses purement techniques ou sectorielles. Elles traversent des domaines, chevauchent des responsabilités, créent des zones grises.

Pour répondre à cette complexité, la cellule doit intégrer des compétences transversales : stratégie, sociologie des organisations, compréhension des systèmes d'acteurs, analyse des représentations.

C'est à cette condition qu'elle pourra détecter les zones d'imprécision ou de recoupement entre périmètres d'action, là où les responsabilités peuvent se chevaucher ou, au contraire, être négligées.

En situation de crise, ces flous deviennent des points de tension. Il faut les cartographier en amont pour définir clairement qui agit, dans quel cadre, et avec quels moyens.

Cette clarification préalable évite blocages, doublons ou angles morts, et permet d'articuler efficacement les contributions au moment décisif.

Faire émerger une culture stratégique

Anticiper est une pratique, mais aussi une culture à construire.

Elle ne se décrète pas : elle s'installe avec le temps, par la répétition, les retours d'expérience, et la valorisation de ceux qui pensent avant d'agir. Elle suppose aussi d'assumer que tout ne se joue pas pendant la crise.

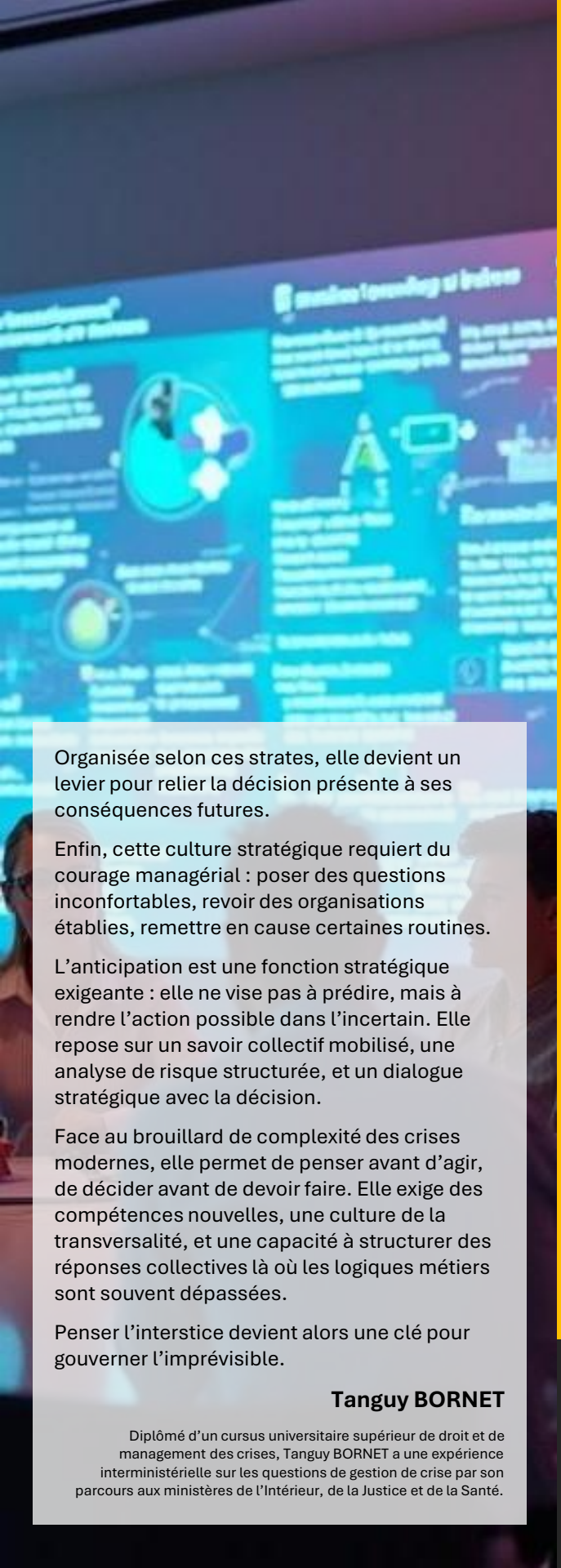
Des décisions structurantes doivent être prises en amont — souvent dans des contextes peu visibles — pour permettre une réponse efficace ensuite. C'est un renversement difficile à faire accepter dans des organisations centrées sur l'action immédiate, mais c'est le prix d'une gouvernance lucide.

L'anticipation s'exerce à plusieurs niveaux :

- **opérationnel**, pour les manœuvres proches du terrain ;
- **tactique**, pour l'allocation des moyens et acteurs ;
- et **stratégique**, pour la lecture globale, les interdépendances et les effets différés.

Ces niveaux doivent être articulés, nourris les uns par les autres, et ancrés dans l'écosystème réel du dispositif de crise : architecture des responsabilités, circuits d'information, acteurs mobilisables.

Sans cet ancrage, l'anticipation reste théorique.



Organisée selon ces strates, elle devient un levier pour relier la décision présente à ses conséquences futures.

Enfin, cette culture stratégique requiert du courage managérial : poser des questions inconfortables, revoir des organisations établies, remettre en cause certaines routines.

L'anticipation est une fonction stratégique exigeante : elle ne vise pas à prédire, mais à rendre l'action possible dans l'incertain. Elle repose sur un savoir collectif mobilisé, une analyse de risque structurée, et un dialogue stratégique avec la décision.

Face au brouillard de complexité des crises modernes, elle permet de penser avant d'agir, de décider avant de devoir faire. Elle exige des compétences nouvelles, une culture de la transversalité, et une capacité à structurer des réponses collectives là où les logiques métiers sont souvent dépassées.

Penser l'interstice devient alors une clé pour gouverner l'imprévisible.

Tanguy BORNET

Diplômé d'un cursus universitaire supérieur de droit et de management des crises, Tanguy BORNET a une expérience interministérielle sur les questions de gestion de crise par son parcours aux ministères de l'Intérieur, de la Justice et de la Santé.

10 astuces d'anticipation pour concourir à la conduite de crise

1. **Cartographier les responsabilités avant d'agir :** Anticiper, c'est d'abord clarifier qui fait quoi, avec qui et comment, pour éviter l'improvisation désordonnée dans l'urgence.
2. **Organiser l'incertain, ne pas le subir :** Anticiper, c'est structurer la réponse possible face à l'imprévisible, en acceptant l'incertitude comme cadre, non comme excuse à l'inaction.
3. **Capitaliser les retours d'expérience… et s'entraîner :** Les expériences vécues, en situation réelle ou simulée, sont des leviers d'apprentissage majeurs. Cette fonction doit être ancrée dans le dispositif réel, via des exercices réguliers et des formations ciblées.
4. **Planifier pour mieux manœuvrer :** La planification n'est pas un enfermement : elle soutient la manœuvre, autorise l'adaptation, et rend pensable l'exception.
5. **Construire une palette de scénarios pour ouvrir le champ des possibles :** Scénarios minorants, médiants ou majorants permettent d'identifier des marges de réponse, de préparer les décisions en amont et de gagner en agilité.
6. **Décider tôt pour permettre d'agir juste au bon moment :** Prévoir, tester, former : autant d'actes invisibles, mais essentiels qui rendent possibles les manœuvres futures.
7. **Ancrer l'anticipation dans un mandat stratégique clair :** La cellule décisionnelle ne valide pas seulement : elle porte la stratégie. Elle a besoin d'un mandat clair pour arbitrer et structurer les choix en amont.
8. **Écouter activement pour mieux éclairer :** L'anticipation doit alimenter la réflexion stratégique de la cellule, en intégrant signaux faibles, tensions et angles morts.
9. **Mobiliser des compétences transversales :** Stratégie, représentation, acteurs : les savoirs transverses complètent l'expertise métier face à la complexité croissante des crises.
10. **Valoriser ceux qui pensent avant d'agir :** Penser avant l'action, c'est déjà agir : c'est une contribution stratégique à part entière, à reconnaître et encourager.

Médiatraining : une parole stratégique pour la gestion de crise

Chaque mot peut faire ou défaire une réputation.

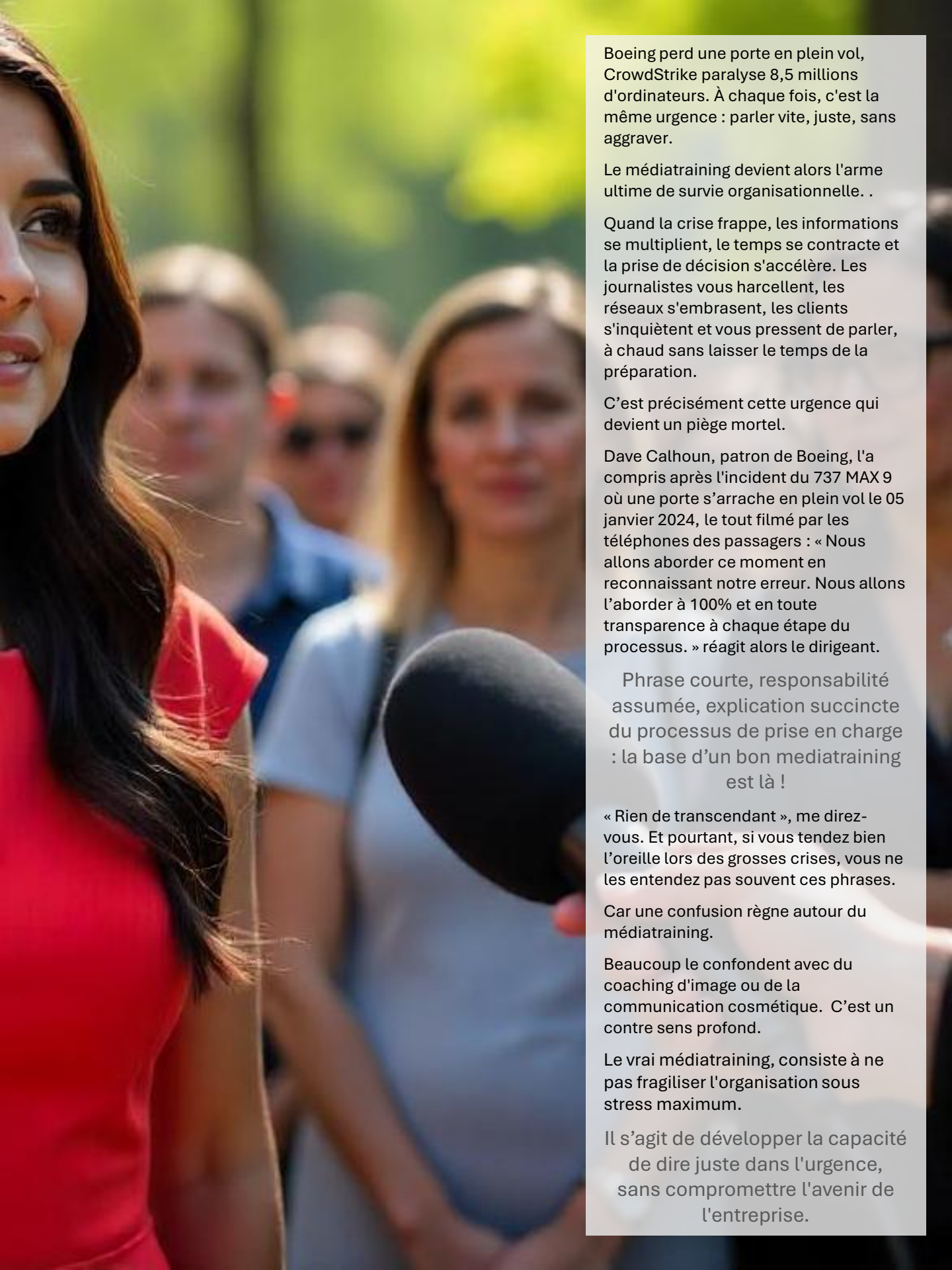
Au moment de la crise, c'est la parole qui détermine la survie ou l'effondrement d'une organisation.

Et c’est là que le médiatraining devient une arme de guerre économique.

Découvrez les techniques essentielles pour transformer vos crises en victoires stratégiques.

Timothy Mirthil de Segonzac

Consultant en prise de parole / media training pour leaders d’influence • Formateur en négociation



Boeing perd une porte en plein vol, CrowdStrike paralyse 8,5 millions d'ordinateurs. À chaque fois, c'est la même urgence : parler vite, juste, sans aggraver.

Le médiatraining devient alors l'arme ultime de survie organisationnelle. .

Quand la crise frappe, les informations se multiplient, le temps se contracte et la prise de décision s'accélère. Les journalistes vous harcellent, les réseaux s'embrasent, les clients s'inquiètent et vous pressent de parler, à chaud sans laisser le temps de la préparation.

C’est précisément cette urgence qui devient un piège mortel.

Dave Calhoun, patron de Boeing, l'a compris après l'incident du 737 MAX 9 où une porte s’arrache en plein vol le 05 janvier 2024, le tout filmé par les téléphones des passagers : « Nous allons aborder ce moment en reconnaissant notre erreur. Nous allons l’aborder à 100% et en toute transparence à chaque étape du processus. » réagit alors le dirigeant.

Phrase courte, responsabilité assumée, explication succincte du processus de prise en charge : la base d’un bon mediatraining est là !

« Rien de transcendant », me direz-vous. Et pourtant, si vous tendez bien l’oreille lors des grosses crises, vous ne les entendez pas souvent ces phrases.

Car une confusion règne autour du médiatraining.

Beaucoup le confondent avec du coaching d'image ou de la communication cosmétique. C’est un contre sens profond.

Le vrai médiatraining, consiste à ne pas fragiliser l'organisation sous stress maximum.

Il s’agit de développer la capacité de dire juste dans l'urgence, sans compromettre l'avenir de l'entreprise.

Le 19 juillet 2024, George Kurtz, PDG de CrowdStrike a dû faire face à une panne mondiale causée par une mise à jour défectueuse du capteur de l'agent Falcon de CrowdStrike qui a mis à terre 8,5 millions de systèmes Windows.

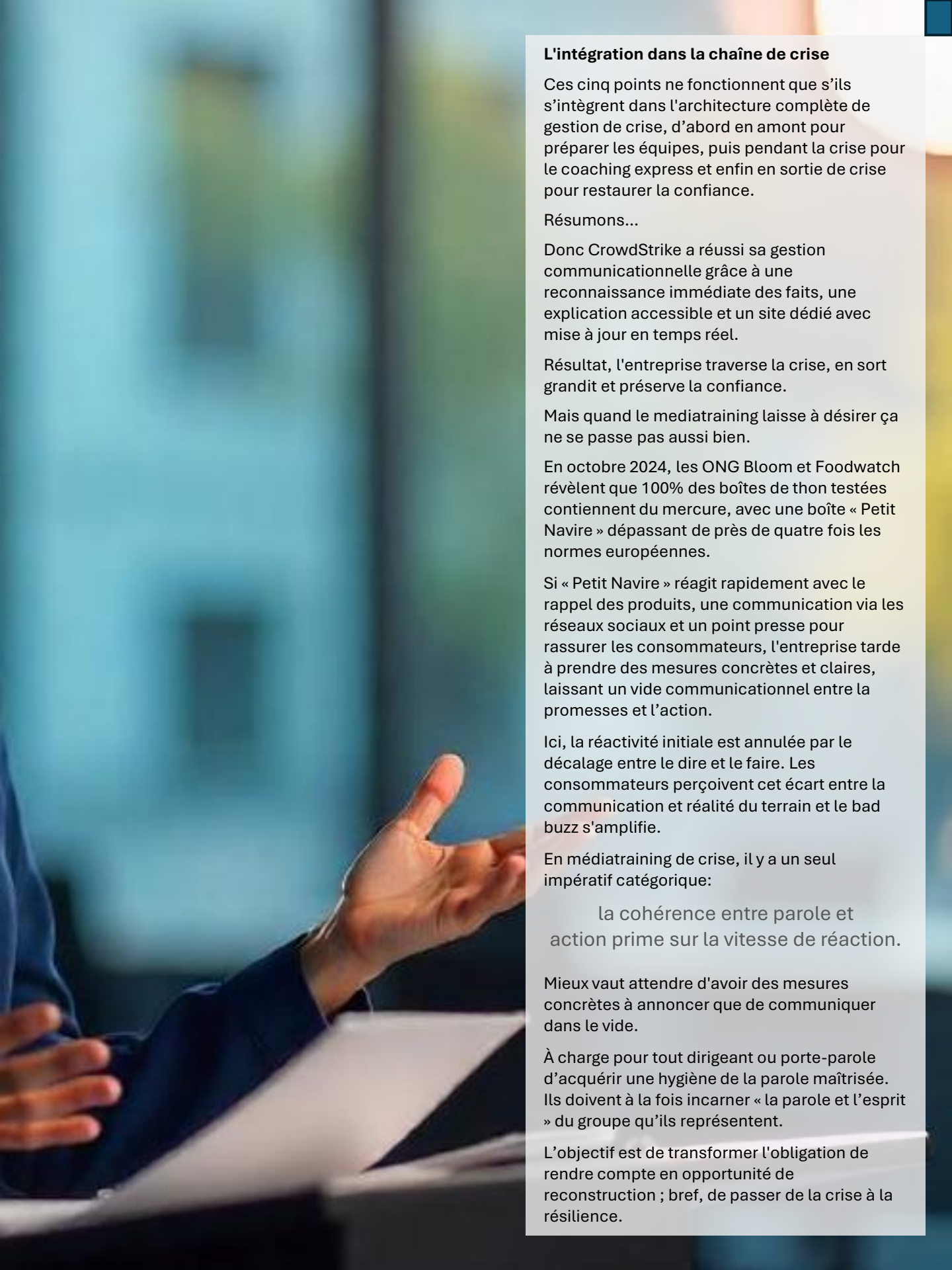
Après des excuses empathiques, le patron de l'entreprise a fourni des détails de la résolution du problème, précisé les moyens déployés, introduit une notion de repères temporels et un surtout proposé un cap clair :

« Nous sommes en train de mettre en place un système d'opt-in pour cette technique. Nous progressons de minute en minute. Nous sommes conscients de l'impact profond que cette situation a eu sur tout le monde. Nous savons que nos clients, nos partenaires et leurs équipes informatiques travaillent sans relâche et nous leur en sommes profondément reconnaissants. Nous nous excusons pour les perturbations que cela a engendrées. Notre objectif est clair : restaurer chaque système *dès que possible*. Nous continuerons à fournir des mises à jour au fur et à mesure que des informations seront disponibles et que de nouveaux correctifs seront déployés ».

Ces phrases qui font la différence entre effondrement et reconstruction.

Pour obtenir cette qualité de message en période de crise, le médiatraining doit certes passer par le pilier de la parole mais pas seulement. Il s'agit de :

- **Garder une présence stable malgré l'hostilité**. L'entraînement passe par des simulations d'interviews agressives en conditions réelles : Posture sous pression.
- **Maîtriser les formules qui apaisent sans compromettre.** "Nous savons que la situation est grave et le désagrément que cela occasionne pour vous. Et nous agissons", devient plus puissant qu'un long discours technique : Empathie et désescalade.
- **Organiser sa pensée sous stress en exposant les faits, l'impact puis l'action**. Jamais plus de trois points par intervention à l'attention de ses équipes : Structure et action.
- **Ne pas laisser l'ego ou la peur décider** grâce aux techniques de respiration contrôlée et de visualisation : Gestion émotionnelle.
- **Ancrer les réflexes** par la mise en situation avec de vrais journalistes ou des contradicteurs formés : Répétition opérationnelle.



L'intégration dans la chaîne de crise

Ces cinq points ne fonctionnent que s'ils s'intègrent dans l'architecture complète de gestion de crise, d'abord en amont pour préparer les équipes, puis pendant la crise pour le coaching express et enfin en sortie de crise pour restaurer la confiance.

Résumons...

Donc CrowdStrike a réussi sa gestion communicationnelle grâce à une reconnaissance immédiate des faits, une explication accessible et un site dédié avec mise à jour en temps réel.

Résultat, l'entreprise traverse la crise, en sort grandit et préserve la confiance.

Mais quand le mediatraining laisse à désirer ça ne se passe pas aussi bien.

En octobre 2024, les ONG Bloom et Foodwatch révèlent que 100% des boîtes de thon testées contiennent du mercure, avec une boîte « Petit Navire » dépassant de près de quatre fois les normes européennes.

Si « Petit Navire » réagit rapidement avec le rappel des produits, une communication via les réseaux sociaux et un point presse pour rassurer les consommateurs, l'entreprise tarde à prendre des mesures concrètes et claires, laissant un vide communicationnel entre la promesses et l'action.

Ici, la réactivité initiale est annulée par le décalage entre le dire et le faire. Les consommateurs perçoivent cet écart entre la communication et réalité du terrain et le bad buzz s'amplifie.

En médiatraining de crise, il y a un seul impératif catégorique:

la cohérence entre parole et action prime sur la vitesse de réaction.

Mieux vaut attendre d'avoir des mesures concrètes à annoncer que de communiquer dans le vide.

À charge pour tout dirigeant ou porte-parole d'acquérir une hygiène de la parole maîtrisée. Ils doivent à la fois incarner « la parole et l'esprit » du groupe qu'ils représentent.

L'objectif est de transformer l'obligation de rendre compte en opportunité de reconstruction ; bref, de passer de la crise à la résilience.

Conclusion :

Le médiatraining ne garantit pas l'absence de polémique, mais une parole qui ne se retourne pas contre l'organisation. Ces trois exemples de crise révèlent que la bataille communicationnelle précède et survit aux autres combats.

Désormais, l'information circule plus vite que la compréhension donc maîtriser sa parole devient un acte éminemment stratégique.

Timothy Mirthil

Ancien journaliste, Timothy Mirthil guide les dirigeants de secteurs sensibles dans l'art de la prise de parole stratégique.

Collaborant avec l'agence TTA, il forme également les cadres exécutifs à la maîtrise des négociations complexes et à l'optimisation de leurs performances par des techniques de bio-hacking.

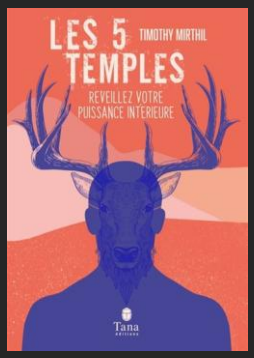
5 clés pour réussir votre médiatraining de crise

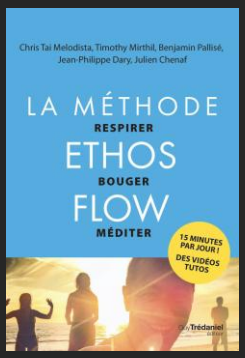
- **1. Préparez votre message principal.** Définissez en une phrase ce que vous voulez absolument faire passer. Mémorisez-la. C'est votre bouée de sauvetage quand l'interview dérape.
- **2. Maîtrisez la règle des trois.** Jamais plus de trois points par intervention : reconnaissance du problème + action engagée + perspective d'amélioration.
- **3. Entraînez-vous sous pression.** Organisez des simulations avec de vrais journalistes ou des collaborateurs formés à jouer les contradicteurs. Répétez jusqu'à ce que vos réponses deviennent fluides, « dans votre bouche».
- **4. Travaillez votre gestuelle :** Position stable, regard direct, mains visibles. Votre corps parle avant vos mots. Un dirigeant dont le « corps s'excuse » inspire moins confiance qu'un dirigeant qui assume avec droiture.
- **5. Anticipez les questions piège**. Listez les cinq questions les plus hostiles possibles sur votre dossier. Préparez des réponses courtes qui reconnaissent sans accuser : « C'est effectivement un point que nous examinons très sérieusement ».

Bonus : Respirez en carré durant 2 minutes avant toute intervention : inspiration sur 4 temps, blocage sur 4 temps, expiration sur 4 temps, blocage sur 4 temps. Vous stabilisez ainsi votre système nerveux autonome et gagnez en concentration et agilité d'esprit.

Le secret : transformez chaque question agressive en opportunité de revenir à votre message principal. « Cette question soulève un point important, et c'est exactement pourquoi nous… », puis vous enchaînez sur votre message essentiel.

À LIRE *DU MÊME AUTEUR …*





L'académie Crise & Résilience

L'unique Académie qui

Renforce votre Cyber Résilience,

une formation à la fois

FORMEZ-VOUS ICI

Code QR de l'académie

www.academiecriseetresilience.com

Stratégie de crise : le pouvoir méconnu de votre alimentation

Lucidité, calme, endurance : qualités essentielles en crise.

N’est-ce pas ?

Pourtant, peu d'organisations adaptent l'alimentation de leurs équipes mobilisées.

Découvrez des recommandations simples pour soutenir les capacités cognitives autrement que par le traditionnel duo "café-sucreries" qui transforme les décideurs en montagnes russes émotionnelles.

Virginie JANTY

Consultante en gestion de crise
et résilience organisationnelle

Gérer une crise mobilise intensément le corps et le cerveau. Pourtant, l'alimentation reste le grand oublié des cellules de crise. Elle est souvent réduite au rang de simple carburant pour transporter votre cerveau d'une réunion d'urgence à l'autre.

Le corps et le cerveau en première ligne

La gestion de crise ressemble à un marathon intellectuel en costume-cravate : vos neurones font des heures sup' sans compensation tandis que votre corps accumule la fatigue.

Dans ces moments critiques, la tentation est grande d'opter pour des solutions immédiates. "Encore un petit café pour tenir?" devient le mantra de ces réunions interminables. Or ces choix sont loin d'être anodins car conditionnent directement votre capacité à rester lucide quand tout s'embrase.

L'effet trompeur du duo café-sucre

Le sucre raffiné, les bonbons, c'est le fameux collègue qui vous promet monts et merveilles avant de vous laisser tomber brutalement.

Ces pics glycémiques suivis de chutes d'énergie transforment votre cerveau en yo-yo métabolique.

Et dans un contexte où chaque décision compte, partir en hypoglycémie au moment crucial n'est pas exactement recommandé dans le manuel des bonnes pratiques de gestion de crise.

La caféine, quant à elle, joue un double jeu très sournois. Stimulante à petite dose, dans un premier temps, elle devient contre-productive en excès en augmentant le cortisol.

Et là, vous passez de décideur calme et réfléchi à pile électrique sur le point d'imploser.

Six expressos plus tard, vos mains se mettent à trembler et votre capacité à rassurer les parties prenantes s'est évaporée en même temps que votre dernier café.

Des choix alimentaires stratégiques pour optimiser les performances décisionnelles

Sans transformer votre cellule de crise en retraite de yoga, voici quelques tactiques alimentaires qui permettront à vos équipes de garder leurs neurones en ordre de bataille :

- **Miser sur l'énergie stable :** remplacez les sucres rapides par des céréales complètes, légumineuses ou fruits secs. C'est la différence entre une Ferrari qui doit s'arrêter toutes les 15 minutes pour faire le plein et un 4x4 qui traverse le désert sans sourciller.

- **Renforcer la résistance au stress :** les aliments riches en magnésium et oméga-3 sont les renforts silencieux qui maintiennent votre cerveau opérationnel quand la situation devient explosive. Ces nutriments jouent un rôle protecteur pour le cerveau face aux situations de stress aigu, comme un bouclier invisible contre la pression.
- **Repenser l'hydratation :** oui, une tisane peut être l'atout secret des leaders les plus respectés – surtout quand elle vous permet de rester lucide après 15 heures de crise quand vos collègues accros au café sont en train de s'effondrer. La camomille n'a jamais compromis le leadership de personne, mais un mauvais call sous l'effet de la caféine, ça oui.
- **Alléger la charge digestive :** les aliments ultra-transformés détournent tellement d'énergie pour la digestion qu'il ne vous reste plus grand-chose pour réfléchir. C'est comme assigner 80% de vos équipes à une tâche secondaire pendant que l'incendie principal dévore les étages stratégiques et menace de faire s'effondrer tout l'édifice.

Repenser l'environnement de crise

Préparer une cellule de crise implique aussi de réfléchir à l'environnement alimentaire proposé à ses membres.

Voyez cela comme l'équipement tactique de votre cerveau : on n'envoie pas des soldats au front avec des armes défectueuses, pourquoi enverriez-vous votre cerveau gérer une crise avec du carburant de mauvaise qualité?

Cette approche n'est pas une lubie de nutritionniste en sandales, mais un véritable levier stratégique qui mérite toute l'attention des gestionnaires de crise.

C'est un élément de performance organisationnelle souvent négligé alors qu'il influence directement la qualité des prises de décision sous pression.

Une alimentation adaptée peut significativement améliorer la concentration, la résistance au stress et la clarté d'esprit - trois éléments cruciaux lorsque chaque décision pèse lourd dans la balance.

Une dimension stratégique souvent négligée

La performance en situation de crise repose autant sur les compétences que sur l'état physiologique des décideurs.

En intégrant des choix alimentaires adaptés, les organisations renforcent significativement leur capacité de réponse collective. Cette approche simple commence par de petits changements mais peut faire toute la différence.

Parce qu'en définitive, le vrai courage managérial, c'est peut-être d'oser troquer sa sixième tasse de café contre une infusion, pour le bien de tous.

Virginie JANTY

Avec 4 ans d'expérience comme formatrice en gestion de crise,j'ai formé plus de 100 chefs d'établissements scolaires pour renforcer la sécurité et la résilience de leurs équipes face aux crises.

RHUYS CONSEIL
ANTICIPER. PROSPÉRER

www.rhuys-conseil.fr

5 choix alimentaires pour performer en cellule de crise

En situation de crise, votre cerveau est comme un moteur de Formule 1 qui tourne à plein régime.

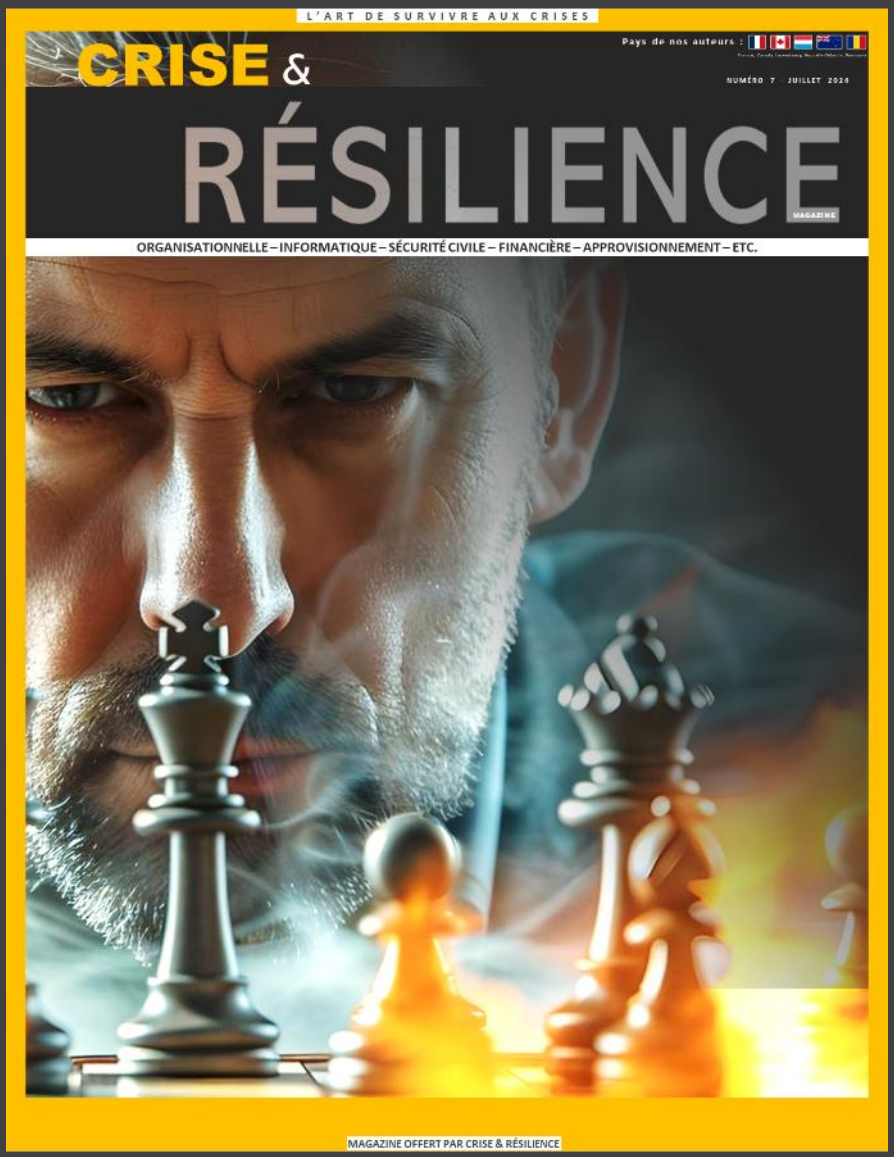
Pour éviter la panne sèche, voici cinq tactiques des meilleurs stratèges :

1. **Prévoir des encas énergétiques et digestes :** remplacez les bonbons par des fruits secs et oléagineux. Ils libèrent leur énergie progressivement, comme un investissement à long terme, plutôt que de flamber votre capital d'attention en 15 minutes.
2. **Repenser l'hydratation :** une tisane n'est pas réservée aux grands-mères enrhumées. Ces boissons chaudes peuvent vous aider à garder votre calme quand la pression monte. Alternez judicieusement entre café et infusions apaisantes pour maintenir votre vigilance sans finir avec les nerfs à vif comme une machine à espresso surchauffée.
3. **Privilégier des repas équilibrés :** optez pour des plats simples à base de protéines maigres et céréales complètes. Votre cerveau consomme 20% de votre énergie - n'envoyez pas le reste au département "digestion de pizza surgelée" en pleine crise.
4. **Créer un espace de respiration alimentaire :** même en pleine tempête, accordez-vous 10 minutes pour manger sans fixer votre écran. Voyez ces minutes comme un rechargement stratégique. Si les meilleurs experts en gestion de crise s'accordent cette pause, vous pouvez le faire aussi.
5. **Intégrer la nutrition à la préparation logistique :** un général prépare sa logistique avant la bataille. Prévoyez des encas intelligents et bannissez les bombes à retardement ultra-transformées. Votre cellule de crise mérite mieux que le distributeur du sous-sol.

Une alimentation stratégiquement pensée fait la différence entre une équipe qui tient bon et une autre qui s'effondre au moment crucial.

Ce n'est pas une mode passagère, c'est de la science appliquée à la performance sous pression.

RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

www.CriseEtResilience-Magazine.com