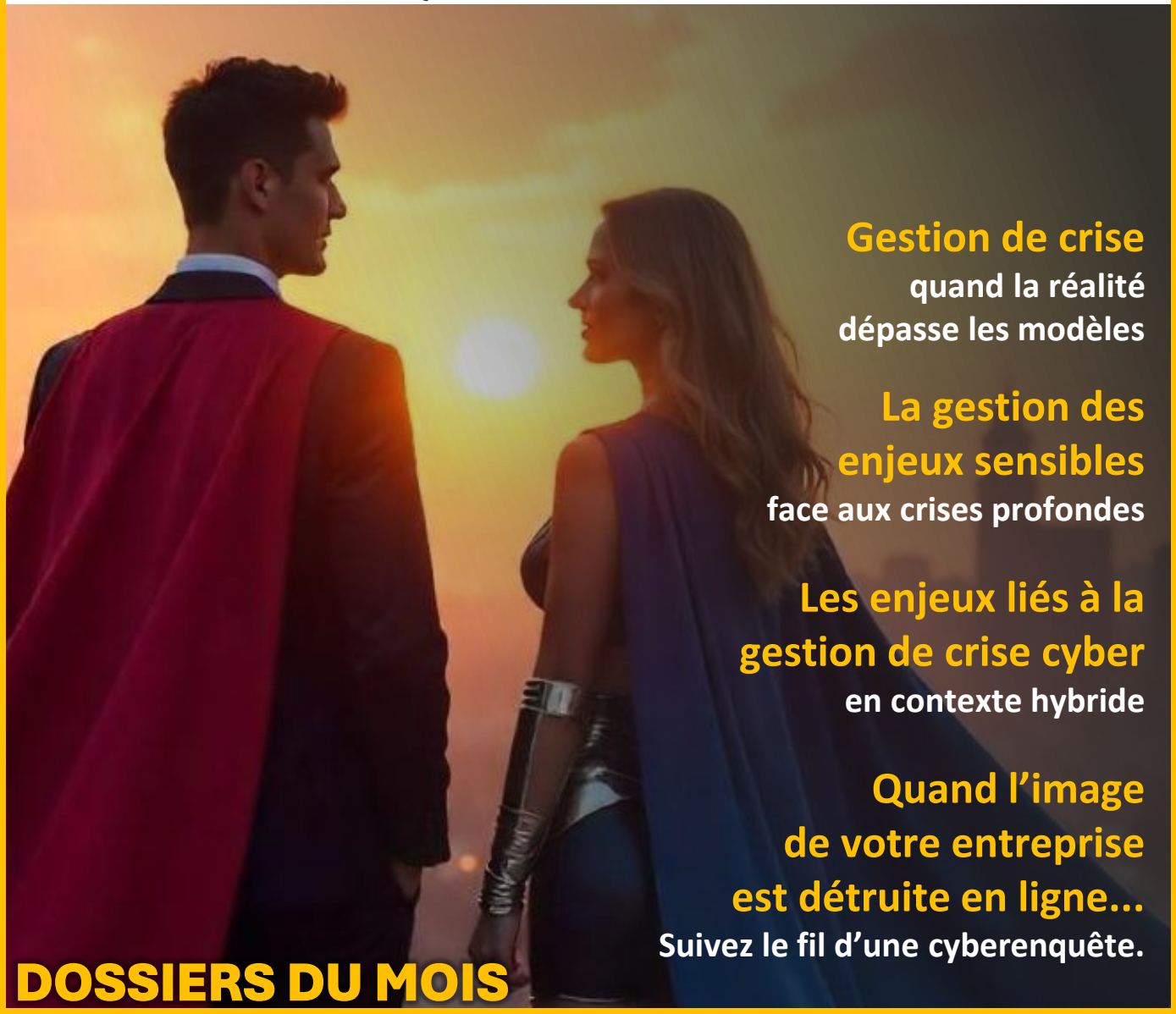
Pays de nos auteurs : France, Canada, Luxembourg, Nouvelle-Zélande, Roumanie, Singapour

CRISE & RÉSILIENCE MAGAZINE

NUMÉRO 9 – Janvier 2025

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



Gestion de crise
quand la réalité dépasse les modèles

La gestion des enjeux sensibles
face aux crises profondes

Les enjeux liés à la gestion de crise cyber
en contexte hybride

Quand l'image de votre entreprise est détruite en ligne...
Suivez le fil d'une cyberenquête.

DOSSIERS DU MOIS

LEADERSHIP
EN TEMPS DE CRISE

MAGAZINE OFFERT PAR CRISE & RÉSILIENCE

Prochaines formations

Académie **Crise & Résilience**

Oui vous avez bien lu...

Nos formations ont une garantie!

www.academiecriseetresilience.com

Édito

Chers lecteurs,

Une nouvelle année, une nouvelle aventure ! Toute l'équipe de Crise & Résilience Magazine vous présente ses meilleurs vœux pour l'année 2025. Qu'elle soit remplie de joie, de bonheur, de santé, de succès et de résilience pour relever tous les défis à venir.

Pour ce premier numéro de l'année, nous attaquons fort avec un thème au cœur de l'actualité : le leadership de crise. Quand tout vacille, seuls des leaders peuvent inspirer, décider vite et transformer chaque crise en levier d'action. Dans notre dossier, partez à la rencontre de leaders qui ont su braver l'impensable. Le leadership de crise, ce n'est pas simplement réagir à l'urgence : c'est anticiper l'inattendu, prendre des décisions rapides et efficaces, et mobiliser les énergies pour avancer. Ce dossier vous révèle les clés d'un leadership solide à travers trois étapes essentielles : prévoir l'imprévisible, agir avec sang-froid sous pression, et rebâtir avec détermination.

Grande nouveauté dans notre magazine ! Nous avons l'immense plaisir d'accueillir Raphaël de Vittoris, qui enrichira chaque trimestre nos pages avec une chronique scientifique incontournable. À travers des analyses pointues et des faits solides, il partagera des thématiques essentielles liées à la gestion de crise.

Et ce n'est pas tout ! Plongez au cœur d'une crise réelle, parce que rien ne vaut l'expérience concrète, nous vous proposons une étude de cas captivante. Analysez une situation réelle, découvrez les erreurs à éviter et appliquez ces enseignements à vos propres défis. Ce contenu pratique est conçu pour renforcer vos compétences face à l'imprévisible.

Un immense merci à tous nos auteurs et contributeurs, véritables éclaireurs de la résilience, qui rendent ce numéro aussi riche qu'inspirant. Grâce à leur expertise et leur passion, vous aurez entre les mains bien plus qu'un magazine : un outil pour progresser et rebondir face à l'imprévu.

Et maintenant ? Prenez l'avantage ! 2025 pourrait être une année chaotique… mais elle peut aussi devenir celle où vous prendrez un temps d'avance. Avec Crise & Résilience Magazine, transformez chaque menace en opportunité.

Bonne lecture, et surtout … bonne résilience !

L'équipe éditoriale

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 !

L'équipe éditoriale

Direction de la publication: Alexandre Fournier
Crédit photo: FreePix, Création IA **Création graphique:** Alfo65
Correction: Véronique Cyr **Édition:** Crise&Résilience, Québec (Qc), CA
Nous contacter : info@crise-resilience.com

Sommaire

Comment échapper à Six erreurs classiques en gestion de crise	Karine Maréchal-Richard	6
Comment organiser une Gestion de crise efficace dans les écoles ?	Virginie Janty	12
Cybersécurité et devoir de prudence et de diligence des administrateurs	Elhadji M. Niang	18
Gestion de crise : Quand la réalité dépasse les modèles	Raphaël de Vittoris	22
Industrie en crise : 5 clés pour une collaboration efficace avec les pompiers	Geoffrey Fillet	28
La gestion des enjeux sensibles face aux crises profondes	Didier Heiderich	34
Les enjeux liés à la gestion de crise cyber en contexte hybride	Adrian Vallecchia	40
Quand l'image de votre entreprise est détruite en ligne… Suivez le fil d'une cyberenquête	Philippe Chevalier	46
Quand le loup… est dans la bergerie	Alexandre Fournier	50
Quelle gouvernance pour capitaliser réellement sur un retour d'expérience post-crise ?	Vamara FOFANA	54
Dossier du mois – Leadership En temps de crise	Karine Maréchal-Richard	60

Participez à un exercice de gestion de crise dans une mise en situation de cyberattaque.

Prochains événements

Janvier à mars 2025

21 janvier – 17 février – 18 mars

17 et 18 février

7 ateliers de mars à avril

14 avril - Soyez présent à ce lancement ! - Méga offre !

Le SéQCure réinventé

une édition incontournable en 2025

Les **26 et 27 février**, le SéQCure revient avec une formule repensée pour offrir des conférences enrichissantes et accessibles à tous les passionnés de cybersécurité.

Cette année, l'événement déménage au cœur du quartier Saint-Roch, à **La Nef**, une salle historique et emblématique. Ce changement stratégique permet une **réduction significative du prix des billets**, rendant l'événement plus abordable, notamment pour la relève. Même si le diner n'est pas inclus dans le prix de base, vous pourrez profiter de restaurants variés à proximité pour satisfaire toutes vos envies culinaires.

Au programme : deux jours de conférences captivantes adaptées aux professionnels et aux curieux du domaine. En présentiel ou à distance, choisissez la formule qui vous convient grâce à notre approche hybride.

Découvrez la programmation et réservez votre place dès maintenant.
https://seqcure.org/

SéQCure

Comment échapper à six erreurs classiques en gestion de crise

Dans un monde où chaque seconde compte, savoir gérer une crise est essentiel.

Quelles sont les six erreurs fatales en gestion de crise qui pourraient freiner votre ascension ?

Découvrez comment les déjouer et transformer chaque défi en une opportunité de croissance.

Ne laissez pas une mauvaise gestion entraver votre succès : prenez les devants dès maintenant.

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.

“Un plan sans pratique, c’est une illusion de « sécurité ».”

Karine Maréchal-Richard

La gestion de crise n'est pas exclusivement l'apanage des experts en risques ou des spécialistes des situations d'urgence.

Chaque organisation, quel que soit son secteur, est susceptible de se retrouver face à une crise.

La capacité de gérer efficacement ces situations peut faire la différence entre une résilience renforcée et un déclin potentiel.

Voici six erreurs fréquemment commises en gestion de crise et des conseils pour les éviter.

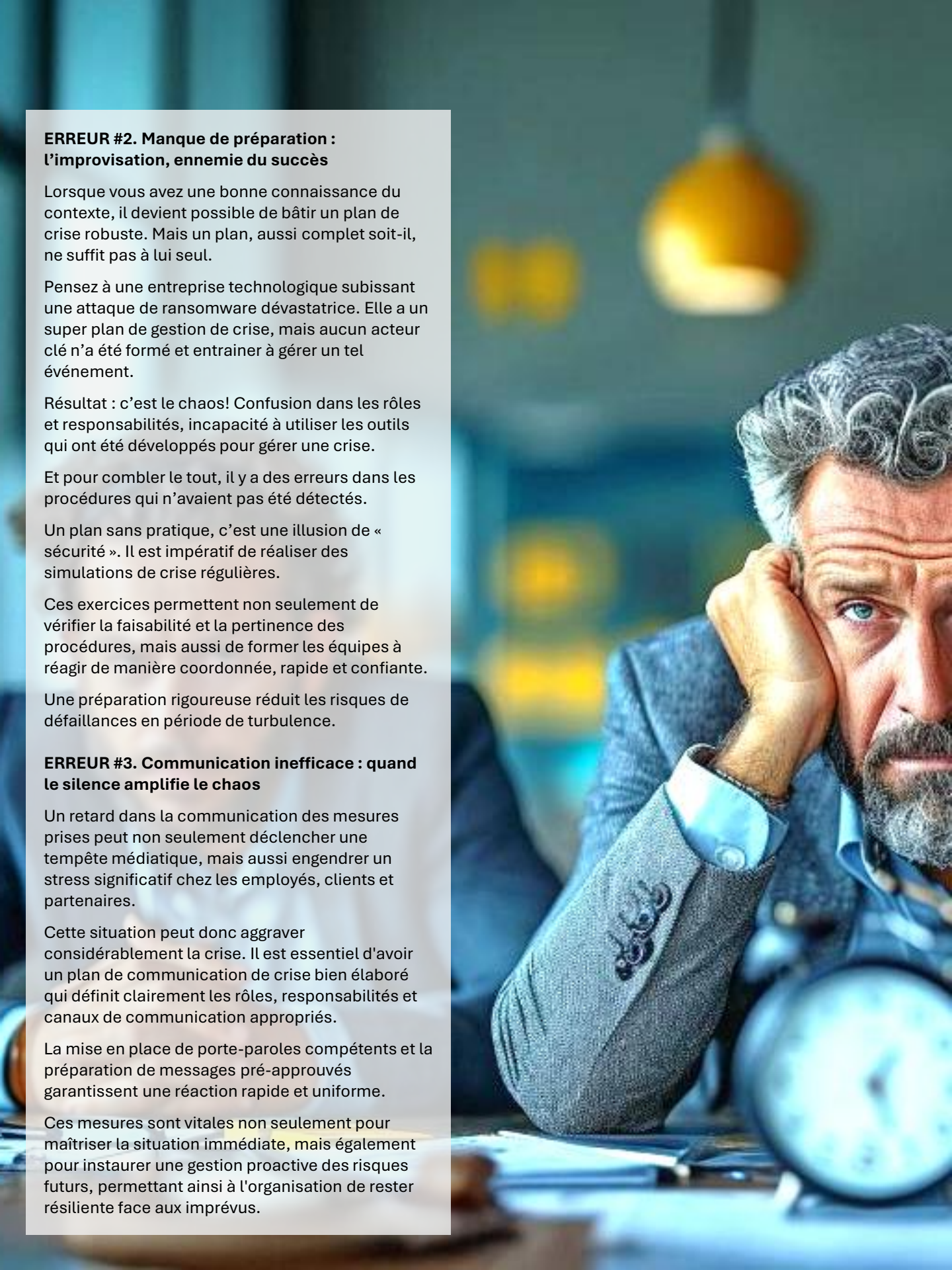
ERREUR #1. Méconnaissance du contexte : l’ignorance qui coûte cher

Imaginez une multinationale qui, en pleine crise sanitaire, réalise trop tard que son principal fournisseur en Asie est incapable de livrer des composants essentiels, entraînant une rupture catastrophique de la chaîne d'approvisionnement.

Pour éviter ces écueils, il est crucial d’investir dans une analyse de risque couvrant les vulnérabilités stratégiques, technologiques et opérationnelles.

Cela implique de mettre en place un système dynamique de surveillance et d’évaluation des risques. Ce système doit garantir que tous les scénarios critiques sont pris en compte et qu'ils correspondent à la réalité évolutive de l'organisation.

De plus, des études montrent que les entreprises qui adaptent continuellement leur stratégie en réponse à l'évolution du contexte global réduisent leurs risques de perturbation de 30% (source : Global Risk Report).



ERREUR #2. Manque de préparation : l'improvisation, ennemie du succès

Lorsque vous avez une bonne connaissance du contexte, il devient possible de bâtir un plan de crise robuste. Mais un plan, aussi complet soit-il, ne suffit pas à lui seul.

Pensez à une entreprise technologique subissant une attaque de ransomware dévastatrice. Elle a un super plan de gestion de crise, mais aucun acteur clé n'a été formé et entrainer à gérer un tel événement.

Résultat : c'est le chaos! Confusion dans les rôles et responsabilités, incapacité à utiliser les outils qui ont été développés pour gérer une crise.

Et pour combler le tout, il y a des erreurs dans les procédures qui n'avaient pas été détectés.

Un plan sans pratique, c'est une illusion de « sécurité ». Il est impératif de réaliser des simulations de crise régulières.

Ces exercices permettent non seulement de vérifier la faisabilité et la pertinence des procédures, mais aussi de former les équipes à réagir de manière coordonnée, rapide et confiante.

Une préparation rigoureuse réduit les risques de défaillances en période de turbulence.

ERREUR #3. Communication inefficace : quand le silence amplifie le chaos

Un retard dans la communication des mesures prises peut non seulement déclencher une tempête médiatique, mais aussi engendrer un stress significatif chez les employés, clients et partenaires.

Cette situation peut donc aggraver considérablement la crise. Il est essentiel d'avoir un plan de communication de crise bien élaboré qui définit clairement les rôles, responsabilités et canaux de communication appropriés.

La mise en place de porte-paroles compétents et la préparation de messages pré-approuvés garantissent une réaction rapide et uniforme.

Ces mesures sont vitales non seulement pour maîtriser la situation immédiate, mais également pour instaurer une gestion proactive des risques futurs, permettant ainsi à l'organisation de rester résiliente face aux imprévus.

ERREUR #4. Réactivité au lieu de proactivité : être toujours en retard

La communication efficace en temps de crise soutient une stratégie proactive plutôt que réactive.

Envisagez les risques d'ajuster tardivement les mesures de sécurité, une situation où des pertes auraient pu être évitées avec une vigilance accrue.

L'intégration d'outils de veille stratégique et de gestion des risques pour anticiper et répondre aux signes avant-coureurs de crises permet à l'entreprise de ne pas seulement réagir, mais de gérer les situations avec assurance.

Cette anticipation proactive renforce l'ensemble du plan de gestion de crise, et elle est intrinsèquement liée à la nécessité de prendre en compte et de soutenir l'aspect humain lors de crises.

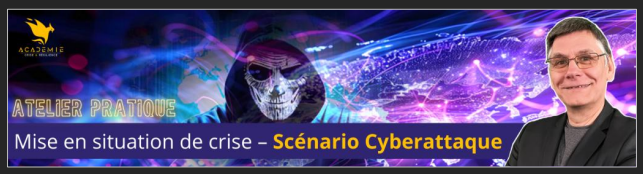
ERREUR #5. Ignorer l'impact humain : l'oubli fatal

En fin de compte, tout plan de gestion de crise doit tenir compte de l'impact humain. Une entreprise qui néglige cet aspect lors d'une crise risque de voir son climat de travail se détériorer.

Intégrer des mesures de soutien pour les employés, telles que des ressources psychologiques, et former les leaders à la communication empathique, garantit non seulement le bien-être des employés mais également le maintien de la productivité en période de crise.

Ce soutien humain enrichit le plan de crise global, soulignant l'importance de tirer des leçons de chaque crise pour améliorer continuellement les stratégies de réponse.

Événements a venir



ERREUR #6. Ne pas tirer les leçons du passé : un cycle de répétition

Chaque crise passée doit servir de leçon pour améliorer les plans futurs. Une entreprise qui répète les mêmes erreurs est condamnée à subir des pertes évitables.

Une analyse post-mortem approfondie après chaque crise permet d'identifier ce qui a bien fonctionné et ce qui doit être amélioré, créant ainsi un cycle vertueux d'amélioration continue qui renforce tous les éléments du plan de gestion de crise, des analyses de risques à la communication et au soutien humain.

Gérer une crise ne se résume pas à réagir ; c'est une affaire de prévoyance, de réactivité et de communication stratégique.

Pour les entreprises visionnaires, les crises ne sont pas des obstacles, mais des tremplins pour l'innovation et la croissance.

En anticipant les risques, en perfectionnant les réponses d'urgence et en valorisant chaque leçon tirée, votre entreprise ne se contente pas de survivre aux tempêtes—elle les maîtrise.

Embrassez la préparation comme une opportunité d'exceller et regardez chaque défi futur comme une chance de prouver votre résilience.

Karine Maréchal-Richard

Consultante et formatrice experte en continuité des affaires et gestion de crise j'accompagne les organisations pour développer leur résilience face aux perturbations majeures.

www.crise-resilience.com

CRISE & RÉSILIENCE
L'ART DE SURVIVRE AUX CRISES

5 clés pour transformer vos erreurs en succès

1. Établissez un plan clair

- Analysez les risques : commencez par identifier les menaces potentielles qui pourraient affecter votre organisation. Cela inclut les risques financiers, opérationnels, technologiques, et environnementaux.
- Formalisez le plan : rédigez un plan de crise qui inclut des protocoles d'action clairs et des responsabilités définies pour chaque membre de l'équipe.

2. Formez vos équipes

- Identifiez les rôles clés : déterminez quels employés joueront un rôle crucial pendant une crise et assurez-vous qu'ils comprennent leurs responsabilités.
- Organisez des formations régulières : mettez en place des sessions de formation régulières pour familiariser vos équipes avec le plan de crise et renforcer leurs compétences en gestion de crise.
- Simulez des crises : effectuez des exercices de simulation pour tester la réactivité et l'efficacité du plan. Cela permet d'identifier les faiblesses et d'améliorer la coordination entre les équipes.

3. Communiquez efficacement

- Élaborez un plan de communication : développez un plan qui spécifie comment l'information sera partagée pendant une crise. Identifiez les canaux de communication appropriés pour chaque public cible (employés, clients, fournisseurs, investisseurs, médias).
- Formez des porte-paroles : choisissez et formez des porte-paroles capables de communiquer clairement et avec assurance pendant une crise.
- Préparez des messages clés : rédigez à l'avance des messages clés qui peuvent être rapidement adaptés et diffusés selon la nature de la crise.

4. Surveillez continuellement

- Implémentez un système de veille : développez des mécanismes pour surveiller en temps réel les indicateurs clés pouvant signaler une crise imminente.
- Analysez les données : évaluez régulièrement les données collectées pour détecter les tendances ou anomalies qui pourraient indiquer un risque accru.
- Réagissez rapidement aux alertes : ayez un protocole en place pour répondre immédiatement aux alertes, minimisant ainsi l'impact potentiel d'une crise.

5. Apprenez des expériences passées

- Effectuez une analyse post-crise : après chaque crise, réalisez une évaluation approfondie pour comprendre ce qui a fonctionné et ce qui doit être amélioré.
- Documentez les leçons apprises : créez un rapport détaillé des leçons apprises et intégrez ces enseignements dans votre plan de gestion de crise.
- Encouragez l'amélioration continue : utilisez ces analyses pour renforcer votre résilience organisationnelle et préparer votre équipe à mieux gérer les crises futures.

Comment organiser une gestion de crise efficace dans les écoles ?

Savoir répondre rapidement et de façon structurée est indispensable en cas de crise en milieu scolaire.

Comment préparer les équipes pour protéger les élèves ainsi que le personnel ?

Découvrez des stratégies concrètes et opérationnelles pour mettre en place une gestion de crise efficace et renforcer la sécurité des établissements scolaires.

Virginie Janty

Fondatrice de Rhuys Conseil - Consultante en gestion de crise spécialiste en gestion de crise et résilience organisationnelle pour les établissements accueillant du public.

Une crise en établissement scolaire revêt un caractère très spécifique. La plus redoutée étant l'intrusion avec violence.

L'anticipation et la préparation sont indispensables.

Des outils adaptés au contexte, une communication fluide et des actions préventives permettent de mieux protéger les élèves, les équipes éducatives et les infrastructures.

1. Pourquoi une gestion de crise bien organisée est essentielle

Les établissements scolaires sont des lieux où la sécurité des biens et des personnes, adultes et enfants, est une priorité pour les dirigeants. En France, c'est la mission première des chefs d'établissement.

De quel type de crise une école, un lycée peut rencontrer ?

- Il peut s'agir d'incidents mineurs comme une bagarre dans la cour ou un retard de livraison des fournisseurs pour le service de cantine.
- Mais il peut se produire des crises majeures comme l'agression d'un personnel ou pire, une tuerie de masse.

Dans tous les cas, il est nécessaire d'avoir une feuille de route claire et structurée afin de limiter les impacts sur la communauté scolaire et d'assurer la continuité pédagogique quand cela est possible.

2. Anticiper les risques pour mieux prévenir

Comme dans toutes les crises, scolaire ou non, la clé d'une gestion de crise réussie réside dans l'anticipation.

La direction connaît normalement assez bien son environnement de travail, qu'il soit question de l'infrastructure ou des personnes.

L'objectif ? Identifier les risques potentiels, même les plus faibles. Les partenaires extérieurs comme les responsables des locaux sont des interlocuteurs privilégiés pour réaliser un audit du bâtiment.

En interne, une bonne connaissance des pratiques et usages de communication entre les personnels est gage de réactivité en cas de problème.

Mais pour rester efficace, il faut être en alerte permanente et ne jamais minimiser le moindre signal faible. Un registre, un cahier, un groupe de discussion dédié peut se révéler un outil précieux pour partager et analyser dans cette phase d'observation.

3. Mettre en place une cellule de crise efficace

L'équipe de direction restreinte peut se considérer comme une cellule de crise.

Pourtant, on se rend compte de l'importance d'une cellule de crise efficace et agrandie quand vient le moment de coordonner les actions et les efforts.

L'objectif est d'être rapidement opérationnel. Chaque minute compte. Des vies sont peut-être en jeu. Pour cela, une équipe doit être spécifiquement dédiée et chacun doit avoir un rôle clairement défini et connu en amont. L'heure n'est plus au questionnement de fonctionnement, mais à l'action.

Cette cellule de crise doit inclure des membres clés de la direction, des enseignants formés.

Une bonne collaboration avec les différents acteurs, notamment les partenaires externes (forces de l'ordre, pompiers, etc.) renforce l'efficacité des réponses.

4. L'importance de la communication en temps de crise

Un établissement scolaire est en communication permanente à l'interne avec les équipes, les élèves, mais aussi avec l'extérieur, avec les familles, les partenaires, les fournisseurs, la presse locale, la municipalité sans oublier l'autorité hiérarchique.

En cas de crise, avoir des canaux de communication spécifiques et adaptés aux pratiques de chacun des interlocuteurs, est crucial pour transmettre un message efficace et rapide.

Pour cela, dans le plan d'action, hiérarchiser les actions de communication permet de n'oublier personne dans la boucle. Prévoir des canaux adaptés et nécessitant le moins d'efforts pour informer les familles, coordonner les équipes enseignantes et maintenir la transparence avec les parties prenantes est une étape essentielle pour éviter les malentendus et contenir les potentiels effets négatifs.

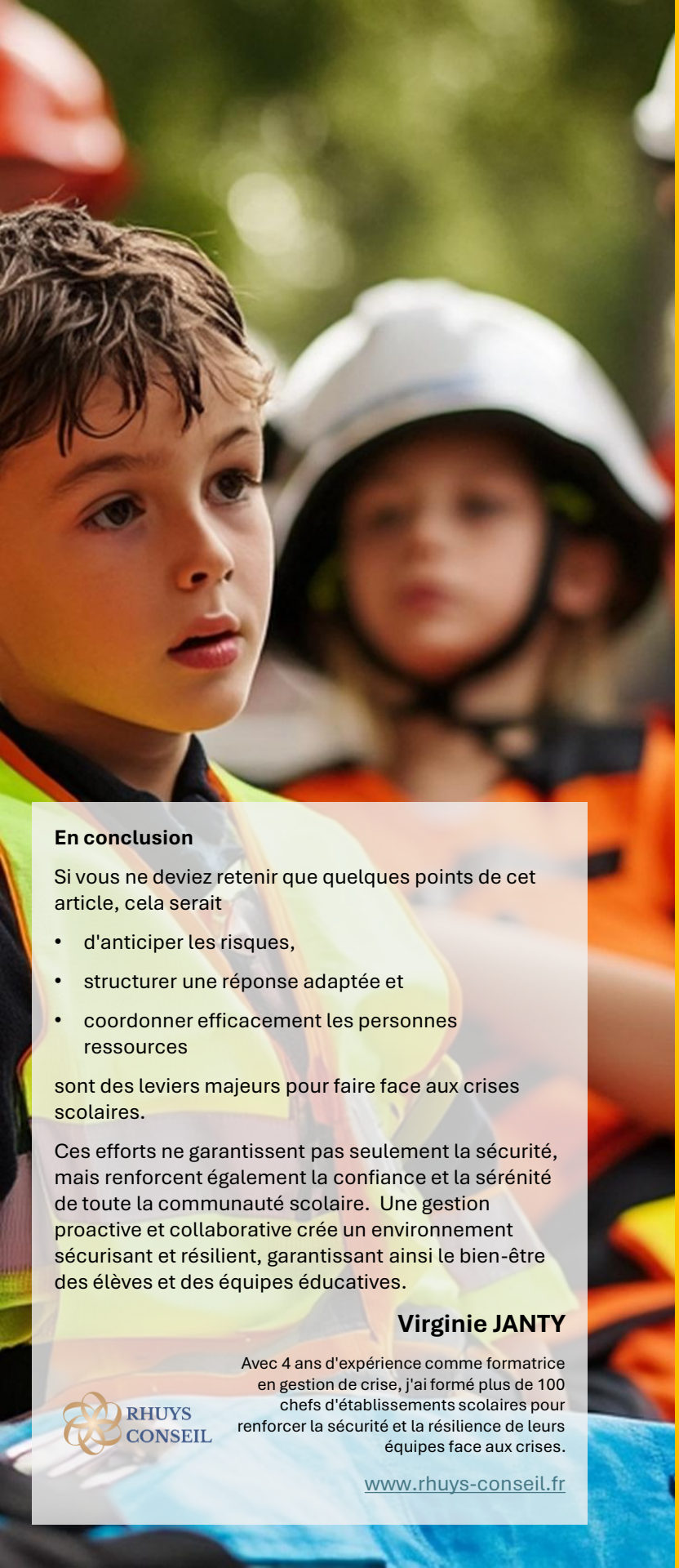
5. Former les équipes et sensibiliser les élèves

Multiplier les exercices de simulations d'urgence, proposer des formations spécifiques aux différentes thématiques (harcèlement, intrusion attentat, risques naturels…) et sensibiliser les élèves, permettent de créer une culture de sécurité dans l'établissement.

C'est en multipliant ces initiatives que les écoles renforcent progressivement leur capacité à gérer les crises et à instaurer un climat de confiance.

Un planning des différents exercices et scénarios utilisés peuvent être décidés en concertation avec les équipes chaque année. Ces temps d'échanges permettent de limiter le côté anxiogène de l'exercice.

C'est souvent pour cette raison que les personnels sont réfractaires à la thématique de la crise. Pourtant écarter ce côté préventif et être dans le déni représente un réel danger pour l'équipe de la cellule de crise en cas de problème.



5 étapes pour un système d'alerte efficace

1. Installez un système d'alerte fiable, spécifique et différent de l'alerte incendie.

Assurez-vous que le dispositif choisi soit accessible par tout le personnel en cas d'urgence. Si vous optez pour un bouton d'alarme, multipliez les points dans l'établissement à des endroits stratégiques.

2. Standardiser les codes d'alerte

Utilisez des signaux d'alerte clairs et universels. Une alarme sonore ou visuelle différente selon la nature du danger : intrusion, incendie, etc.). Ces codes doivent être faciles à comprendre, y compris pour les élèves. Se concerter avec les municipalités pour harmoniser les alertes.

3. Former les équipes à l'utilisation

Organisez des formations régulières pour que chaque membre de l'établissement sache déclencher et interpréter le signal d'alerte en fonction du protocole d'urgence.

4. Tester le système lors de simulations fréquentes

Intégrez systématiquement le système d'alerte aux exercices de simulation afin de vérifier son efficacité en conditions réelles. Ces tests permettent également de repérer d'éventuelles failles (pannes techniques, signal mal compris, etc.).

5. Impliquer les élèves et les familles

Sensibilisez les élèves à reconnaître les signaux d'alerte et à réagir correctement. N'attendez pas 3 mois après la rentrée pour diffuser les différents systèmes d'alertes et les actions attendues. Informez également les familles des protocoles pour qu'elles sachent quoi faire et éviter la panique en cas de crise.

Pourquoi un système d'alerte est essentiel ?

Un bon système d'alerte réduit le temps de réaction face à une crise majeure, il protège les élèves et les équipes, garantissant une coordination rapide avec les forces de l'ordre. Il est un élément clé pour protéger efficacement les biens et les personnes.

En conclusion

Si vous ne deviez retenir que quelques points de cet article, cela serait

- d'anticiper les risques,
- structurer une réponse adaptée et
- coordonner efficacement les personnes ressources

sont des leviers majeurs pour faire face aux crises scolaires.

Ces efforts ne garantissent pas seulement la sécurité, mais renforcent également la confiance et la sérénité de toute la communauté scolaire. Une gestion proactive et collaborative crée un environnement sécurisant et résilient, garantissant ainsi le bien-être des élèves et des équipes éducatives.

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

www.rhuys-conseil.fr

FORMATION

Intégrez l'IA dans la Gestion de Crise

18-19 février 2025

Québec 8h à 12h | France 14h à 18h

FORMATION EN DIRECT VIA TEAMS

Anticipez aujourd'hui, surpassez demain.

Inscrivez-vous dès maintenant pour garantir votre place !

Profitez de notre ...

GARANTIE SATISFAIT OU REMBOURSÉ*

👉www.academiecriseetresilience.com/integrer-ia-et-gestion-de-crise

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

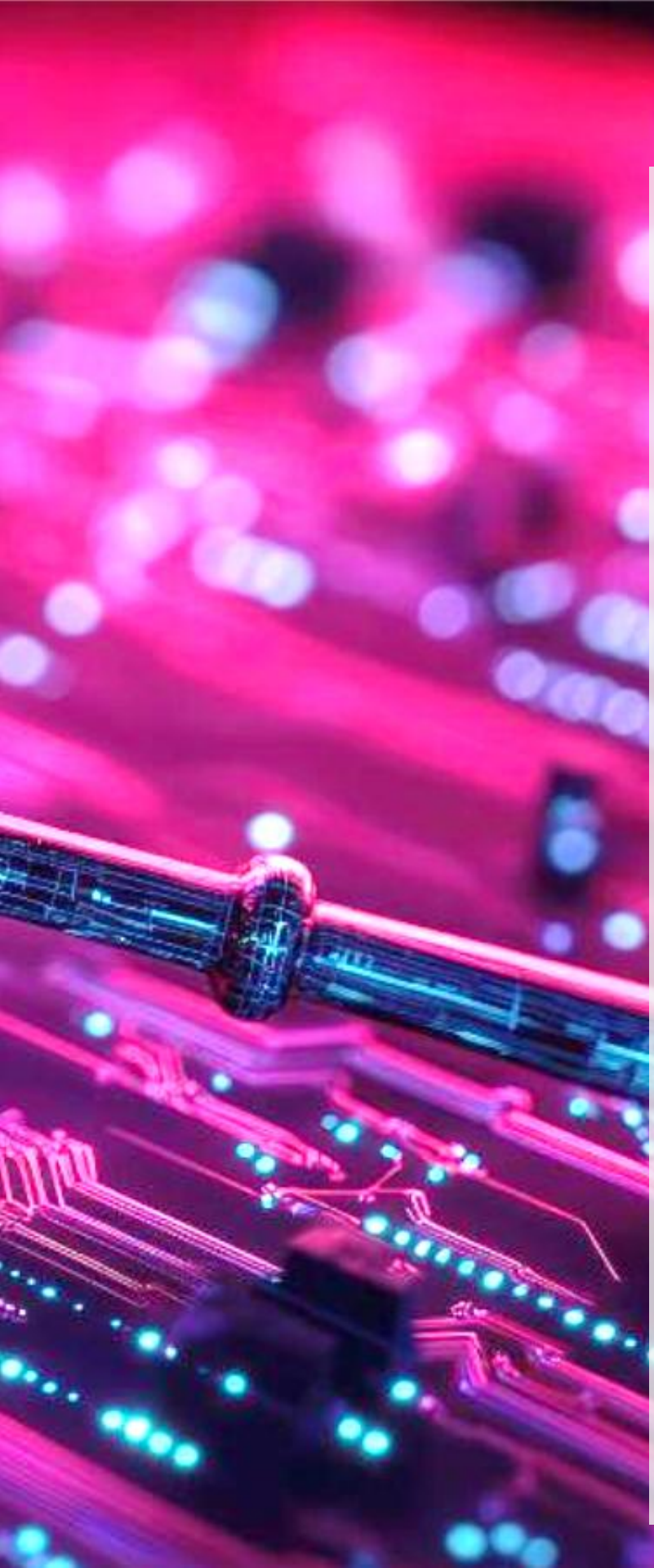
Cybersécurité et devoir de prudence et de diligence des administrateurs.

Selon **Pensez cybersécurité**[1] , « En 2024, la question n'est pas de savoir si les cyberattaques se produiront, mais bien quand elles se produiront… »

Cet article aborde le devoir de prudence et de diligence des administrateurs, face aux risques de cybersécurité, résilience et gestion de crise.

Elhadji M. Niang

Avocat – Conseiller en sécurité de l'information
Droit des technologies - Gouvernance et architecture de sécurité - Protection des renseignements personnels



Sauf exception (convention unanime d'actionnaires[2]), les administrateurs sont responsables des actes de gestion de l'entreprise.

Face à l'accroissement exponentiel des risques de cybersécurité, quelles sont leurs obligations pour prévenir ces attaques et préparer l'entreprise à y réagir ?

I. Que signifie l'obligation de prudence et de diligence de l'administrateur d'une entreprise ?

L'obligation des administrateurs d'agir avec prudence et diligence dans la gestion d'une entreprise est encadrée par plusieurs textes[3]. L'article 322 du Code civil du Québec :

« L'administrateur doit agir avec prudence et diligence. Il doit aussi agir avec honnêteté et loyauté dans l'intérêt de la personne morale. »

Cette obligation de portée générale est aussi reprise par la Loi sur les sociétés par action article 119 et par l'article 122 (1) de la Loi Canadienne sur les sociétés par action.

L'obligation de prudence et de diligence exige des administrateurs et dirigeants de gérer l'entreprise en « bon père de famille », de s'informer adéquatement ou de recourir à des experts pour les éclairer sur des sujets complexes.

La jurisprudence interprète cette obligation comme une obligation de moyen et non comme une obligation de résultats. En effet, il ne s'agit pas de savoir si les administrateurs ont pris la meilleure décision mais si la décision prise revêt les caractéristiques d'une décision de gestion raisonnable compte tenu des circonstances.

Dans le contexte des enjeux de cybersécurité et de résilience, l'obligation de prudence et de diligence peut être analysée sous deux angles :

- En regard des obligations des administrateurs vis-à-vis de l'entreprise,
- En regard du régime général de la responsabilité civile.

II. Obligation de prudence et de diligence des administrateurs et dirigeants en cybersécurité et résilience de l'entreprise

Les entreprises ont une grande dépendance envers les technologies de l'information. Elles sont de plus en plus exposées à des risques dont la réalisation peut avoir de graves conséquences sur la survie de l'entreprise(4).

Il ne s'agit pas de dire ici que les dirigeants et administrateurs doivent développer des compétences spécifiques en matière de cybersécurité.

Il est toutefois de leur devoir de s'assurer que l'entreprise a mis en œuvre les mesures de sécurité raisonnables(5) afin de prévenir et réagir aux cyberattaques visant à paralyser ses activités économiques.

Faute d'y voir, notre opinion est à l'effet que sous l'angle spécifique du devoir de prudence et de diligence, les administrateurs font défaut d'agir dans les meilleurs intérêts de l'entreprise.

III. Obligation de prudence et de diligence sous l'angle de la responsabilité civile de l'entreprise

Nous analysons ici l'obligation de prudence et de diligence des administrateurs en regard au régime général de l'article 1457 du Code civil du Québec qui dispose :

« Toute personne a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages ou la loi, s'imposent à elle, de manière à ne pas causer de préjudice à autrui.

Elle est, lorsqu'elle est douée de raison et qu'elle manque à ce devoir, responsable du préjudice qu'elle cause par cette faute à autrui et tenue de réparer ce préjudice, qu'il soit corporel, moral ou matériel.

Elle est aussi tenue, en certains cas, de réparer le préjudice causé à autrui par le fait ou la faute d'une autre personne ou par le fait des biens qu'elle a sous sa garde. ».

Références :

(1) https://www.pensezcybersecurite.gc.ca/fr/sont-organisations-canadiennes-matiere-cybersecurite-2024

(2) Art. 213 Loi sur les sociétés par actions du Québec

(3) Dans l'affaire Magasins à rayons Peoples inc. (Syndic de) c. Wise, la Cour suprême du Canada nous enseigne au sujet de l'obligation de prudence et de diligence des administrateurs : « La norme de diligence est une norme objective. Les décisions des administrateurs et des dirigeants doivent constituer des décisions d'affaires raisonnables compte tenu de toutes les circonstances, notamment les conditions socio-économiques existantes, qu'ils connaissaient ou auraient dû connaître » - [Soulignement ajouté]

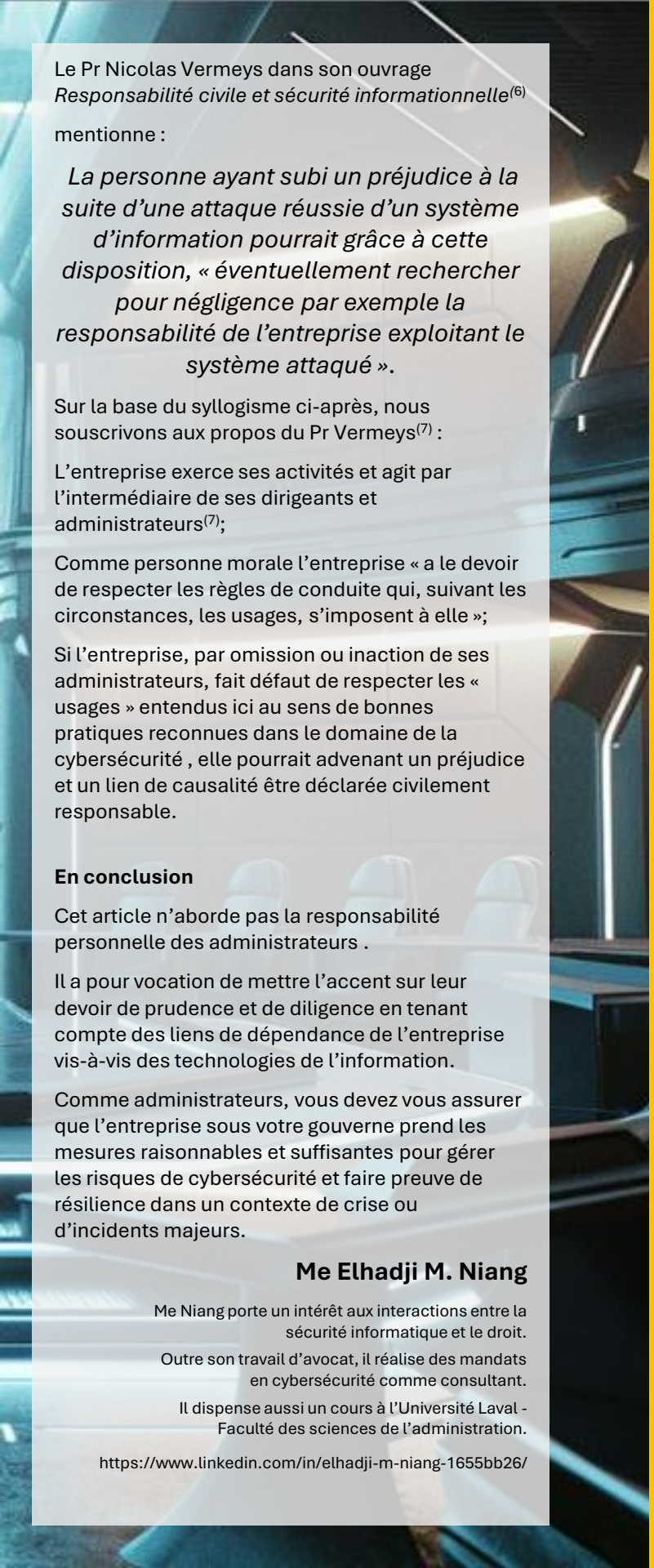
(4) Selon Statistiques Canada : *« En 2023, les dépenses totales engagées pour le rétablissement des activités à la suite d'incidents de cybersécurité ont aussi augmenté. Elles ont doublé pour passer d'environ 600 millions de dollars en 2021 à 1,2 milliard de dollars en 2023. »* Voir https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-fra.htm

(5) Cette obligation de prendre des mesures de sécurité raisonnable est aussi prévue à l'art 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé* et à l'art 63.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

(6) VERMEYS, Nicolas, W., Responsabilité civile et sécurité informationnelle, Cowansville, Yvon Blais, 2010, P. 105

(7) Voir art 311 et 312 du Code civil du Québec

(8)mÀ titre d'exemple seulement, norme ISO 27002 : https://www.iso.org/fr/standard/75652.html , NIST Cybersecurity Framework: https://www.nist.gov/cyberframework , ANSSI : Sécuriser son organisation - https://cyber.gouv.fr/securiser-son-organisation - Centre Canadien pour la cybersécurité : https://www.cyber.gc.ca/fr/petites-moyennes-entreprises



Le Pr Nicolas Vermeys dans son ouvrage *Responsabilité civile et sécurité informationnelle*[6] mentionne :

La personne ayant subi un préjudice à la suite d'une attaque réussie d'un système d'information pourrait grâce à cette disposition, « éventuellement rechercher pour négligence par exemple la responsabilité de l'entreprise exploitant le système attaqué ».

Sur la base du syllogisme ci-après, nous souscrivons aux propos du Pr Vermeys[7] :

L'entreprise exerce ses activités et agit par l'intermédiaire de ses dirigeants et administrateurs[7];

Comme personne morale l'entreprise « a le devoir de respecter les règles de conduite qui, suivant les circonstances, les usages, s'imposent à elle »;

Si l'entreprise, par omission ou inaction de ses administrateurs, fait défaut de respecter les « usages » entendus ici au sens de bonnes pratiques reconnues dans le domaine de la cybersécurité , elle pourrait advenant un préjudice et un lien de causalité être déclarée civilement responsable.

En conclusion

Cet article n'aborde pas la responsabilité personnelle des administrateurs .

Il a pour vocation de mettre l'accent sur leur devoir de prudence et de diligence en tenant compte des liens de dépendance de l'entreprise vis-à-vis des technologies de l'information.

Comme administrateurs, vous devez vous assurer que l'entreprise sous votre gouverne prend les mesures raisonnables et suffisantes pour gérer les risques de cybersécurité et faire preuve de résilience dans un contexte de crise ou d'incidents majeurs.

Me Elhadji M. Niang

Me Niang porte un intérêt aux interactions entre la sécurité informatique et le droit.

Outre son travail d'avocat, il réalise des mandats en cybersécurité comme consultant.

Il dispense aussi un cours à l'Université Laval - Faculté des sciences de l'administration.

https://www.linkedin.com/in/elhadji-m-niang-1655bb26/

3 clés pratiques de cybersécurité pour administrateurs

À titre d'administrateurs, vous devez être en mesure de démontrer avoir fait preuve de diligence et de prudence dans vos actes de gestion.

Voici 3 clés pratiques pour vous acquitter de votre obligation de prudence et de diligence en matière de cybersécurité.

1.Gouvernance

- S'assurer que les encadrements nécessaires (politiques, directives, processus et procédures ...) sont mis en place afin de fixer les orientations, les principes directeurs et règles en matière de cybersécurité.
- Approuver les budgets cybersécurité ainsi que la structure organisationnelle de l'entreprise (répartition des rôles et responsabilités).
- Mesurer la performance (les dépenses de cybersécurité sont justifiées et réduisent les risques) – Amélioration continue et reddition de compte.

2.Gestion des risques

- S'assurer que votre entreprise dispose d'une stratégie et des outils de gestion des risques.
- Exiger minimalement un suivi et une reddition sur les points suivants :
  - Les risques majeurs sont analysés et les mesures de mitigations appropriées sont mises en œuvre;
  - Surveillance des actifs critiques de l'entreprise afin de détecter et réagir en temps opportun à une attaque ou panne.

3.Préparez votre entreprise au pire

La sécurité absolue n'existe pas. En votre qualité d'administrateurs, vous devez-vous assurer :

- Votre entreprise est préparée pour prévenir et réagir aux cyberattaques ou pannes majeurs
- Votre entreprise dispose d'une infrastructure de relève, des copies de sauvegarde et un plan de continuité des activités.
- Votre stratégie de gestion de crise, votre plan de relève informatique et plan de continuité des activités sont régulièrement testés et ils fonctionnent convenablement.

Gestion de crise : quand la réalité dépasse les modèles(1)

Quand la crise frappe, les modèles ne suffisent pas.

Découvrez comment le sensemaking, révélé lors d'une simulation à l'usine Michelin d'Olsztyn, transcende les approches théoriques pour maîtriser l'imprévu.

Une immersion dans la complexité de la gestion de crise où chaque décision compte.

(1) Cros, S., et de Vittoris, R. (2019). Apprendre à favoriser les apprentissages entre acteurs privés et publics : cas d'un site Michelin. Gestion 2000, 36(5), 41-66.

Raphaël de Vittoris

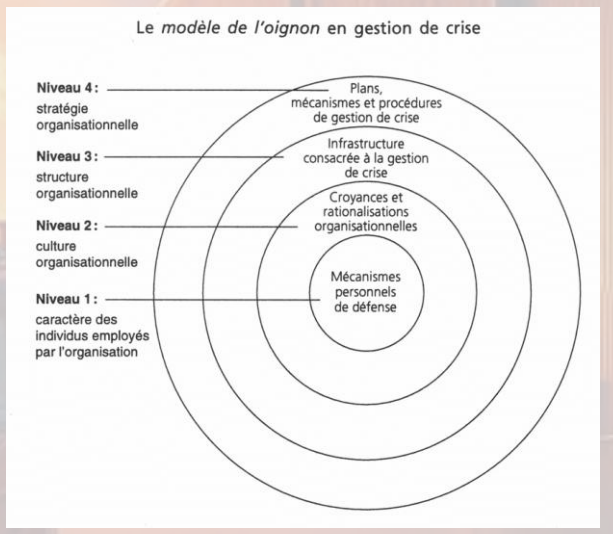
Symbio Director Risk Management / Internal Control / Progress / Cyber / Security – Associate Professor Strategy & Crisis Mgt – Founder Antifragile.fr

L’exercice de simulation mené en 2017 à l’usine Michelin d’Olsztyn, en Pologne, n’était pas une simple répétition.

C’était une immersion dans la complexité de la gestion de crise, un test grandeur nature où chaque décision pouvait faire la différence entre une catastrophe maîtrisée et un chaos incontrôlable.

Employant près de 4 000 personnes et produisant plus de 8 millions de pneus par an, l’usine, située au cœur d’une ville de 180 000 habitants, visait à tester la collaboration des équipes et des forces d’intervention face à un incendie majeur.

La simulation, soigneusement orchestrée, incluait des urgences, des informations inutiles mais stressantes, et des décisions à prendre en temps réel. À première vue, tout respectait les modèles traditionnels de gestion de crise, comme le modèle de l’oignon de Mitroff et d’Anagnos, centré sur la maturité organisationnelle via cinq facteurs clés : facteurs technologiques, structure organisationnelle, facteurs humains, culture organisationnelle et psychologie du top management.



Cependant, cette simulation a montré que la gestion de crise ne se résume pas à cocher des cases sur un modèle théorique.

Malgré la préparation conforme à ces principes, les décisions prises par la direction de l’usine ont eu un impact bien plus crucial que les simples préparatifs matériels ou organisationnels.

La limite du modèle

Le modèle de l'oignon, malgré sa rigueur et sa profondeur, montre ses limites lorsqu'il s'agit d'évaluer la qualité des décisions prises en temps de crise.

Ce modèle se concentre sur la préparation structurelle, mais il ne tient pas compte du facteur humain crucial qu'est la prise de décision sous pression. En d'autres termes, il suppose que, si une organisation est bien préparée sur les cinq axes, elle est prête à faire face à une crise.

Mais l'expérience montre que ce n'est pas toujours le cas.

Prenons un exemple concret de la simulation : l'incendie simulé dans une zone de sous-traitance de l'usine.

En théorie, les portes coupe-feu, si elles avaient été vérifiées, auraient pu contenir l'incendie. Pourtant, aucune vérification n'a été effectuée dans les premières minutes critiques de l'incident.

Résultat?

Une propagation incontrôlée des flammes dans un bâtiment adjacent, et un décès potentiel dans le scénario.

La preuve dans le tableau ci-dessous : l'observation de l'organisation de crise selon les axes du modèle de Mitroff et d'Anagnos montrait un niveau de maturité élevé, alors que nombre des choix opérés par les cellules de crise respectives (celles de l'usine et celle des pompiers de la ville d'Olsztyn) se sont révélés inadaptés.

Facteurs du modèle	Éléments observés	Niveau de maturité considéré
Facteurs technologiques	• *Outils de communication* • *Équipement de la salle de crise*	Élevé
Structure organisationnelle	• *Répartition des rôles* • *Revues périodiques* • *Usage du manuel de crise*	Satisfaisant
Facteurs humains	• *Propension à la communication avec les pompiers de la ville* • *Absence de conflit*	Élevé
Organisation culturelle	• *Anticipation* • *Communication interne et externe* • *Facilitation (via time keeping et aide-mémoire)* • *Partage via le journal de bord* • *Réaction face aux perturbations*	Satisfaisant
Psychologie du *top management*	• *Leadership* • *Priorités claires* • *Volonté de coopération avec la cellule des pompiers de la ville*	Élevé

Cette situation met en lumière un aspect crucial que le modèle de Mitroff et d'Anagnos néglige : la qualité des décisions prises par les dirigeants sur le terrain.

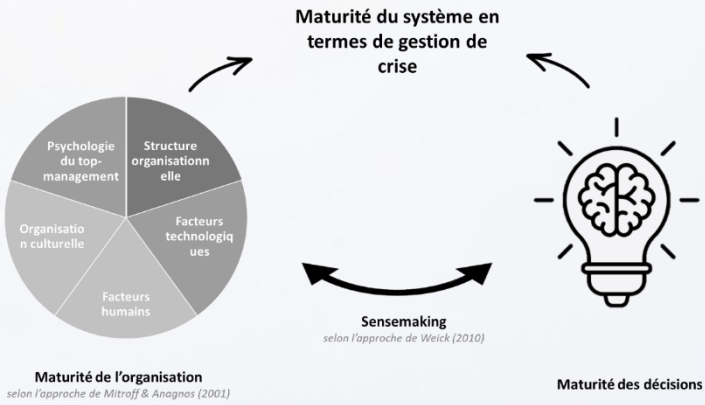
Même avec une infrastructure parfaitement alignée sur le modèle, une mauvaise décision ou une décision tardive peut transformer une situation gérable en une catastrophe. Cela montre que le modèle de l'oignon, bien qu'utile, est incomplet, car il ignore l'aspect dynamique et imprévisible des prises de décision en temps réel.

Le pouvoir du *sensemaking*

C'est ici que le concept de sensemaking entre en jeu. Le sensemaking[2], ou construction de sens, est le processus par lequel les acteurs d'une organisation interprètent les événements et prennent des décisions en temps réel. C'est un pont essentiel entre la préparation théorique et l'action pratique. Sans sensemaking, même la meilleure préparation structurelle peut échouer.

Dans la simulation d'Olsztyn, le sensemaking a permis à la cellule de crise de l'usine de s'adapter à une situation en constante évolution. Par exemple, lorsque l'incendie s'est propagé et que les premières interventions ont échoué, c'est le sensemaking qui a permis à l'équipe de reconfigurer sa stratégie et de gérer les informations contradictoires et stressantes qui affluaient. Il ne s'agissait pas seulement de suivre un plan, mais de comprendre et d'interpréter les événements et d'y réagir de manière cohérente et efficace.

Le sensemaking, dans ce contexte, a permis de dépasser les limites du modèle de Mitroff et d'Anagnos. En reliant les cinq facteurs du modèle à la qualité des décisions prises, il a permis à l'organisation de se montrer résiliente face à la crise. C'est cette capacité à donner du sens aux événements qui a permis à l'équipe de direction de passer d'une simple gestion de crise à une véritable maîtrise de la situation.



[2] *Weick, K. E. (2010). Reflections on enacted sensemaking in the Bhopal disaster. Journal of Management Studies, 47(3), 537-550.*

Conclusion : vers une gestion de crise plus holistique

L'une des principales conclusions de cette simulation est que la maturité d'une organisation en gestion de crise ne peut pas être jugée uniquement sur la base de sa préparation structurelle. La maturité doit également prendre en compte la qualité des décisions prises et la capacité de l'organisation à faire du sensemaking.

L'expérience de l'usine Michelin d'Olsztyn montre que la gestion de crise doit évoluer au-delà des modèles théoriques traditionnels.

Si le modèle de l'oignon de Mitroff et d'Anagnos reste un outil précieux pour évaluer la préparation organisationnelle, il est insuffisant pour garantir la résilience en temps de crise.

La clé réside dans le sensemaking, cette capacité à interpréter les événements en temps réel et à prendre des décisions éclairées et adaptées.

En intégrant le sensemaking et en reconnaissant l'importance cruciale des décisions prises sous pression, les organisations peuvent, en plus de se préparer à une crise, s'assurer qu'elles sont capables de la maîtriser lorsque l'imprévu frappe.

La gestion de crise devient alors non seulement une question d'outils et de plans, mais surtout une question de discernement, de réactivité et d'intelligence collective en action.

Raphaël De Vittoris

Directeur de la gestion des risques, de la gestion de crise, du contrôle interne, du progrès et de la cyberdéfense de l'entreprise Symbio, Raphaël De Vittoris est aussi professeur et chercheur associé en stratégie, en organisation, en management, en gestion de crise et en communication de crise à l'IAE Clermont Auvergne. Il est aussi le fondateur d'Antifragile.fr, qui accompagne les organisations privées et publiques dans la consolidation de leur pérennité. Il est docteur en sciences de gestion et qualifié maître de conférences, diplômé d'un master en physiologie et en environnement extrême, d'un master en administration des entreprises et d'un master en hygiène, sécurité et environnement.

Il est en outre l'auteur de **Surmonter les crises : idées reçues et vraies pistes pour les entreprises** (Dunod, 2021) de **Par-delà la résilience et l'antifragilité : l'entreprise du XXIe siècle** (ESKA, 2022) et de **Déjouer les risques** (DUNOD 2023) .

ANTIFRAGILE.FR

https://antifragile.fr/

À LIRE

DU MÊME AUTEUR ...

Académie **Crise & Résilience**

FORMATION

Mettre en place un Plan de gestion de crise cyber

19 au 23 mai 2025

Québec 8h à 12h | France 14h à 18h

FORMATION EN DIRECT VIA TEAMS

Soyez prêt à gérer la prochaine cyberattaque!

Inscrivez-vous dès maintenant pour garantir votre place !

Profitez de notre ...

GARANTIE SATISFAIT OU REMBOURSÉ*

👉www.academiecriseetresilience.com/plan-de-gestion-de-crisecyber

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

Industrie en crise : 5 clés pour une collaboration efficace avec les pompiers

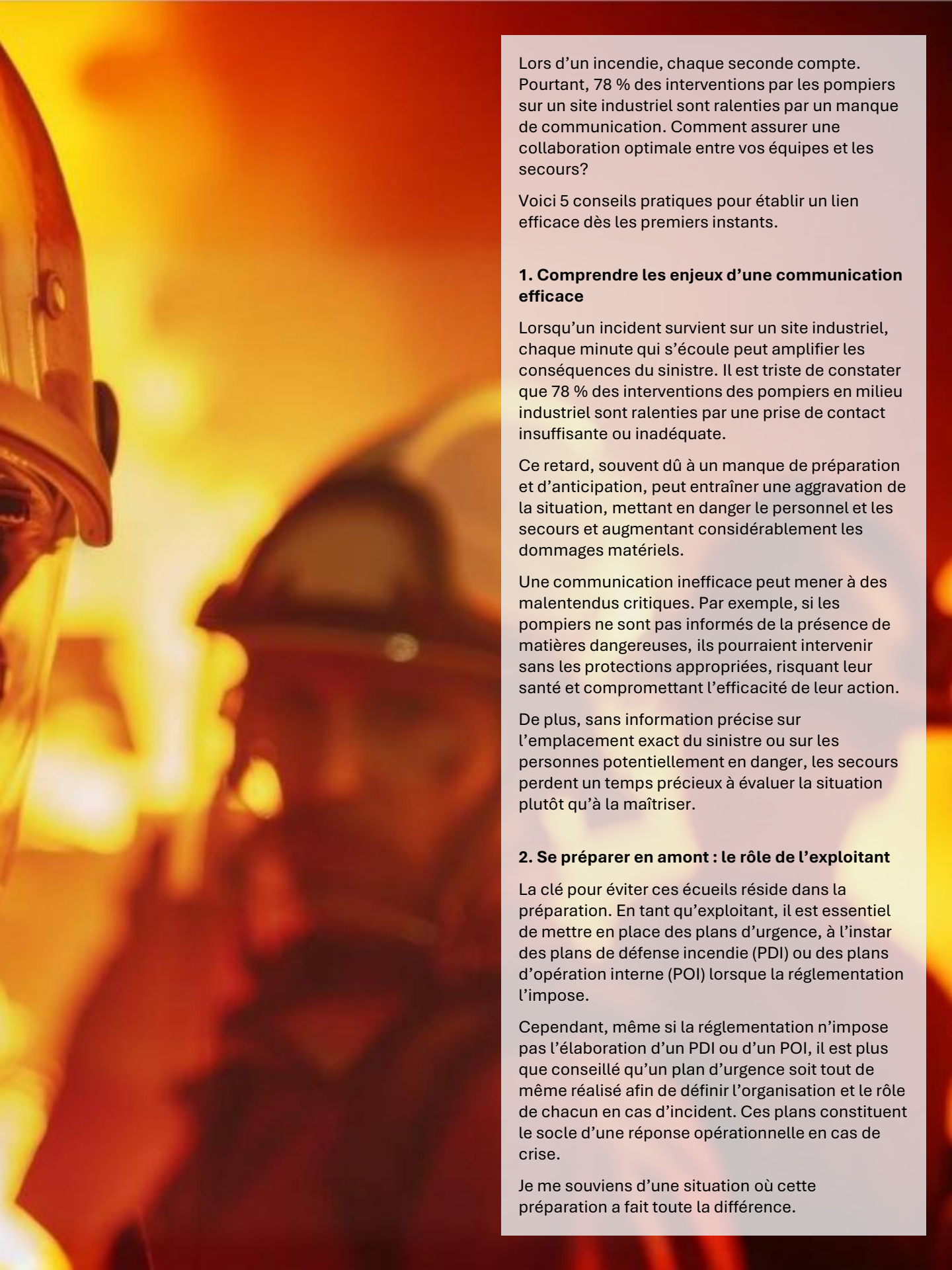
Imaginez votre usine en proie aux flammes. Les pompiers arrivent, mais perdent de précieuses minutes faute d'informations claires.

Trop souvent, une mauvaise communication ralentit leur intervention.

Découvrez comment devenir un véritable facilitateur pour optimiser l'efficacité des secours lors d'un incident industriel.

Geoffrey Fillet

Fondateur et gérant du cabinet Krisis Conseil
Consultant et formateur en gestion et communication de crise



Lors d’un incendie, chaque seconde compte. Pourtant, 78 % des interventions par les pompiers sur un site industriel sont ralenties par un manque de communication. Comment assurer une collaboration optimale entre vos équipes et les secours?

Voici 5 conseils pratiques pour établir un lien efficace dès les premiers instants.

1. Comprendre les enjeux d’une communication efficace

Lorsqu’un incident survient sur un site industriel, chaque minute qui s’écoule peut amplifier les conséquences du sinistre. Il est triste de constater que 78 % des interventions des pompiers en milieu industriel sont ralenties par une prise de contact insuffisante ou inadéquate.

Ce retard, souvent dû à un manque de préparation et d’anticipation, peut entraîner une aggravation de la situation, mettant en danger le personnel et les secours et augmentant considérablement les dommages matériels.

Une communication inefficace peut mener à des malentendus critiques. Par exemple, si les pompiers ne sont pas informés de la présence de matières dangereuses, ils pourraient intervenir sans les protections appropriées, risquant leur santé et compromettant l’efficacité de leur action.

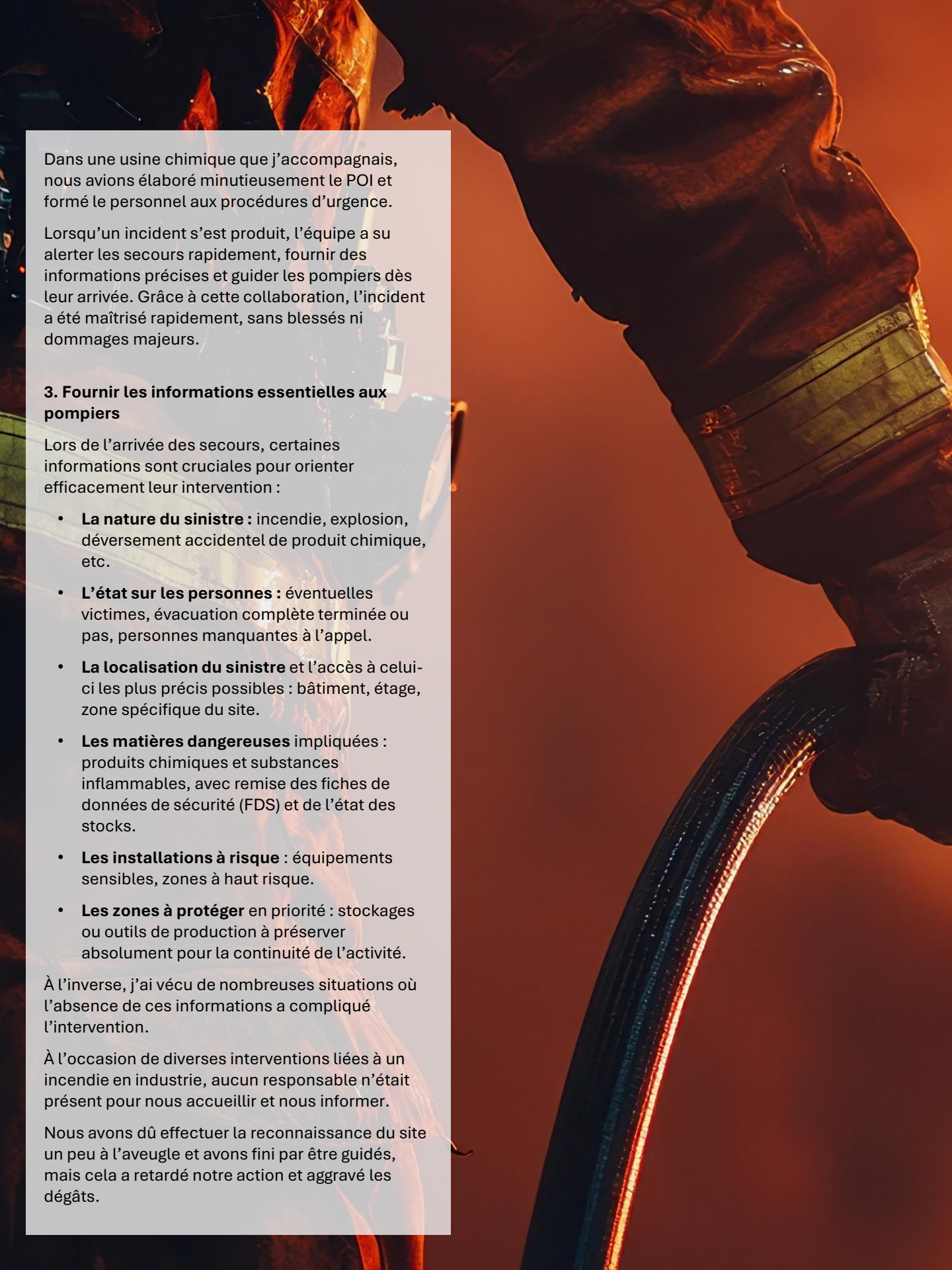
De plus, sans information précise sur l’emplacement exact du sinistre ou sur les personnes potentiellement en danger, les secours perdent un temps précieux à évaluer la situation plutôt qu’à la maîtriser.

2. Se préparer en amont : le rôle de l’exploitant

La clé pour éviter ces écueils réside dans la préparation. En tant qu’exploitant, il est essentiel de mettre en place des plans d’urgence, à l’instar des plans de défense incendie (PDI) ou des plans d’opération interne (POI) lorsque la réglementation l’impose.

Cependant, même si la réglementation n’impose pas l’élaboration d’un PDI ou d’un POI, il est plus que conseillé qu’un plan d’urgence soit tout de même réalisé afin de définir l’organisation et le rôle de chacun en cas d’incident. Ces plans constituent le socle d’une réponse opérationnelle en cas de crise.

Je me souviens d’une situation où cette préparation a fait toute la différence.



Dans une usine chimique que j'accompagnais, nous avions élaboré minutieusement le POI et formé le personnel aux procédures d'urgence.

Lorsqu'un incident s'est produit, l'équipe a su alerter les secours rapidement, fournir des informations précises et guider les pompiers dès leur arrivée. Grâce à cette collaboration, l'incident a été maîtrisé rapidement, sans blessés ni dommages majeurs.

3. Fournir les informations essentielles aux pompiers

Lors de l'arrivée des secours, certaines informations sont cruciales pour orienter efficacement leur intervention :

- **La nature du sinistre :** incendie, explosion, déversement accidentel de produit chimique, etc.
- **L'état sur les personnes :** éventuelles victimes, évacuation complète terminée ou pas, personnes manquantes à l'appel.
- **La localisation du sinistre** et l'accès à celui-ci les plus précis possibles : bâtiment, étage, zone spécifique du site.
- **Les matières dangereuses** impliquées : produits chimiques et substances inflammables, avec remise des fiches de données de sécurité (FDS) et de l'état des stocks.
- **Les installations à risque** : équipements sensibles, zones à haut risque.
- **Les zones à protéger** en priorité : stockages ou outils de production à préserver absolument pour la continuité de l'activité.

À l'inverse, j'ai vécu de nombreuses situations où l'absence de ces informations a compliqué l'intervention.

À l'occasion de diverses interventions liées à un incendie en industrie, aucun responsable n'était présent pour nous accueillir et nous informer.

Nous avons dû effectuer la reconnaissance du site un peu à l'aveugle et avons fini par être guidés, mais cela a retardé notre action et aggravé les dégâts.

4. Faciliter l’accès et la circulation sur le site

Un autre aspect crucial est l’accessibilité du site pour les secours. Les voies d’accès doivent être clairement signalées et dégagées de tout obstacle.

La mise à disposition de plans détaillés du site indiquant les points d’entrée, les emplacements des bornes d’incendie, les organes de coupure (électricité, eau, gaz) et les zones de stockage de matières dangereuses est indispensable.

La présence d’une personne formée pour accueillir les pompiers facilite grandement leur intervention.

Cette personne doit être en mesure de :

- Transmettre les plans et les fiches scénarios d’incidents;
- Fournir des clés ou des badges d’accès aux différentes zones du site;
- Guider les secours jusqu’au lieu du sinistre par l’accès le plus approprié.

Cette collaboration réduit le temps d’intervention et accroît la sécurité de tous.

5. Maintenir une communication continue pendant l'intervention

La communication ne doit pas s'arrêter à la transmission initiale des informations. Tout au long de l'intervention, il est essentiel de maintenir un échange fluide entre l'exploitant et les secours. Pour ce faire :

- Utilisez des moyens de communication adaptés : mettez à disposition des talkies-walkies ou des radios compatibles avec celles des pompiers;
- Restez disponible : un représentant de l'entreprise doit être présent pour répondre aux questions techniques ou fournir des informations complémentaires;
- Anticipez les besoins des secours : par exemple, préparez les plans d'évacuation, les schémas des installations ou les procédures de mise en sécurité.

Cette communication continue permet aux pompiers d'adapter leur stratégie en temps réel et d'agir plus efficacement.

Préparez-vous et impliquez vos équipes pour améliorer votre résilience!

En établissant un contact efficace avec les pompiers, vous maximisez les chances de limiter les impacts d'un incident sur votre site. Cette collaboration est essentielle pour la sécurité de vos employés et la préservation de vos installations. Ne laissez pas le hasard dicter la gestion de la situation de crise.

Geoffrey FILLET

Geoffrey Fillet a effectué un parcours professionnel diversifié dans le domaine de la sécurité et de la gestion des risques tant dans le secteur public que dans le secteur privé. Sapeur-pompier de Paris et pompier professionnel durant 16 ans, puis chargé en hygiène, en sécurité et en environnement dans l'industrie, il a ensuite été responsable du service sécurité-sûreté au sein d'un centre hospitalier.

Il met aujourd'hui à profit ses 20 années d'expérience terrain auprès des organisations en les aidant à gagner en sérénité tout en se recentrant sur l'importance et la force des collaborateurs.

En 3 ans, il a accompagné plus de 40 entités, leur permettant d'aborder efficacement et le plus sereinement possible les situations imprévisibles.

KRISIS CONSEIL

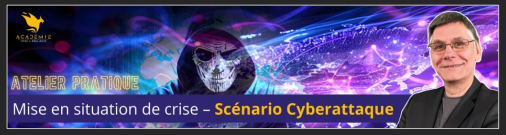
https://krisisconseil.fr/

Guide pratique : accueillir les pompiers en 7 étapes clés

1. Préparez un point de situation précis : décrivez l'incident, les zones touchées, les risques spécifiques.
2. Remettez les plans du site et les procédures d'urgence : incluez-y les emplacements des équipements de sécurité.
3. Indiquez le meilleur accès au sinistre : assurez-vous que les voies sont dégagées et accessibles.
4. Fournissez des moyens de communication : mettez à disposition des talkies-walkies ou des radios compatibles.
5. Signalez les zones à risques particuliers : matières dangereuses, installations à risque.
6. Identifiez les zones à protéger en priorité : zones stratégiques pour la continuité d'activité.
7. Restez disponible pour les pompiers : une personne compétente doit accompagner les secours tout au long de l'intervention.

En appliquant ces étapes, vous facilitez l'intervention des secours et contribuez à une gestion de crise efficace.

Événements a venir



Académie Crise & Résilience

FORMATION

Mettre en place un Plan de continuité des activités

24 au 28 novembre 2025

Québec 8h à 12h | France 14h à 18h

FORMATION EN DIRECT VIA TEAMS

Maintenez vos activités essentielles pour survivre à la crise!

Inscrivez-vous dès maintenant pour garantir votre place !

Profitez de notre ...

GARANTIE SATISFAIT OU REMBOURSÉ*

👉www.academiecriseetresilience.com/plan-de-continuite-des-activites

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

La gestion des enjeux sensibles face aux crises profondes

Dans les années 2000, Nokia dominait le marché des téléphones mobiles avec des produits innovants et une forte présence sur le marché.

Cependant, l'entreprise a été confrontée à un bouleversement technologique qui a conduit à sa chute : la gestion des enjeux sensibles se destinent à anticiper et gérer ces crises majeures.

Didier Heiderich

Ingénieur, physicien-chimiste, président de l'Observatoire International des Crises, fondateur HEIDERICH Consultants

Historiquement, la gestion de crise vise à contenir les impacts d'une crise et à restaurer la normalité rapidement.

Cependant, dans un monde en mutation, cette approche réactive montre ses limites. Les organisations doivent adopter une stratégie anticipative pour gérer les enjeux sensibles et éviter qu'ils ne deviennent des crises majeures.

Les enjeux sensibles : une menace insidieuse et puissante

Contrairement aux crises soudaines, les enjeux sensibles émergent progressivement. Ils naissent de mutations internes ou de transformations externes comme l'évolution des normes sociales, des controverses sociétales, ou encore de l'introduction de technologies de rupture.

Exemple : L'intelligence artificielle (IA)

Initialement perçue comme une innovation prometteuse, l'IA est rapidement devenue un enjeu sensible. Si elle offre des opportunités de croissance, elle soulève des questions éthiques : impact sur l'emploi, protection des données ou biais algorithmiques. Une entreprise adoptant l'IA sans anticiper ces défis risque une crise de réputation ou des régulations plus strictes.

Gérer ces enjeux nécessite une stratégie à long terme, basée sur une compréhension approfondie des dynamiques en jeu. Il ne s'agit pas simplement de réagir, mais d'anticiper, de structurer et de mettre en place des actions concrètes pour atténuer les risques et les impacts.

Pourquoi intégrer la gestion des enjeux sensibles ?

Les enjeux sensibles ne se limitent pas à des risques isolés. Leur gestion proactive permet de naviguer dans un environnement de plus en plus complexe et interconnecté. En anticipant ces défis, les organisations peuvent :

- Identifier les signes avant-coureurs de crises potentielles.
- Protéger leur réputation et renforcer l'autorisation sociale d'exercer.
- Adapter leurs pratiques aux attentes croissantes des parties prenantes.
- Préparer les situations de crise.

Exemple : La consommation responsable

L'évolution des attentes sociétales en matière d'éthique et de durabilité a transformé l'industrie alimentaire. Les entreprises ayant anticipé ces changements ont renforcé leur position sur le marché, tandis que celles qui les ont ignorés ont subi des critiques publiques et des pertes de confiance.

Pendant la crise : gérer l'effet domino et l'effet de halo

Lorsqu'une crise éclate, deux phénomènes amplifient souvent ses impacts : l'effet domino et l'effet de halo.

- **L'effet domino :** Une crise initiale entraîne une cascade d'événements. Par exemple, une cyberattaque peut paralyser les systèmes internes, affecter les fournisseurs, et générer une méfiance durable chez les clients.
- **L'effet de halo :** Une erreur ou un incident peut nuire à l'image globale de l'organisation. Par exemple, une collectivité mal préparée à une catastrophe naturelle, comme à Valence lors des inondations de novembre 2024, peut voir sa capacité à gérer d'autres crises remise en question.

Prévenir ces effets :

- Identifier les interdépendances critiques et anticiper les scénarios possibles.
- Communiquer rapidement pour éviter les perceptions négatives durables.
- Agir de manière coordonnée pour limiter les impacts secondaires.

La cellule de crise : un levier stratégique

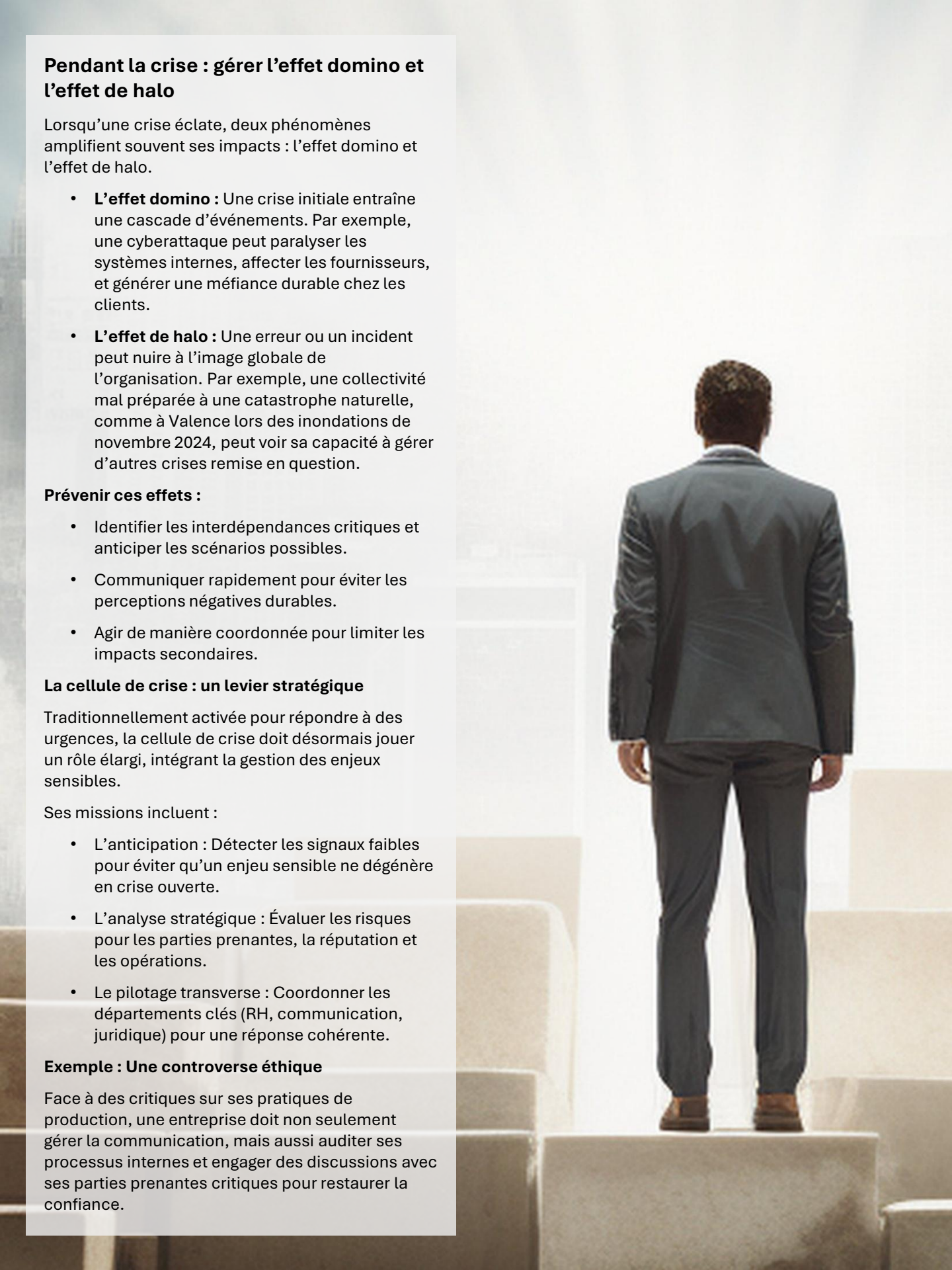
Traditionnellement activée pour répondre à des urgences, la cellule de crise doit désormais jouer un rôle élargi, intégrant la gestion des enjeux sensibles.

Ses missions incluent :

- L'anticipation : Détecter les signaux faibles pour éviter qu'un enjeu sensible ne dégénère en crise ouverte.
- L'analyse stratégique : Évaluer les risques pour les parties prenantes, la réputation et les opérations.
- Le pilotage transverse : Coordonner les départements clés (RH, communication, juridique) pour une réponse cohérente.

Exemple : Une controverse éthique

Face à des critiques sur ses pratiques de production, une entreprise doit non seulement gérer la communication, mais aussi auditer ses processus internes et engager des discussions avec ses parties prenantes critiques pour restaurer la confiance.



Après la crise : transformer les enjeux en opportunités

Chaque crise offre une occasion d'apprendre et d'évoluer. Une gestion proactive des enjeux sensibles permet de :

- Renforcer la résilience organisationnelle.
- Transformer les défis en opportunités stratégiques.
- Restaurer la confiance en démontrant une capacité d'adaptation.

Exemple : La transition énergétique

Dans l'industrie automobile, les acteurs ayant anticipé le passage aux véhicules électriques dominent aujourd'hui le marché.

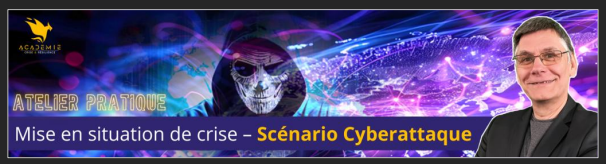
Ceux qui ont tardé à s'adapter subissent des pertes face à des concurrents plus innovants.

Vers une résilience accrue grâce à la gestion des enjeux sensibles

La résilience organisationnelle est bien plus qu'une simple capacité à surmonter les crises : c'est un état d'être, une posture durable qui repose sur l'aptitude à anticiper, à s'adapter et à prospérer dans un environnement marqué par l'incertitude et le changement constant.

Dans ce contexte, la gestion des enjeux sensibles émerge comme un levier central, permettant aux organisations de renforcer leur résilience et de mieux appréhender un monde où les crises sont souvent complexes, interconnectées et amplifiées par les dynamiques globales.

Événements a venir



La gestion des enjeux sensibles comme une opportunité face aux crises profondes

Naviguer dans les enjeux sensibles et les crises profondes nécessite anticipation, réactivité et stratégie.

Amplifiées par les évolutions normatives, technologiques et idéologiques, ces crises ne peuvent être gérées uniquement de manière réactive. Bien qu'insidieux, les enjeux sensibles peuvent devenir des leviers d'innovation et de résilience.

En adoptant une vision globale, en menant une veille active et en cartographiant les risques, les organisations transforment ces défis en opportunités stratégiques.

Cette gestion proactive permet de prévenir les crises, de renforcer leur position et de préparer un avenir durable et résilient.

Didier Heiderich

Didier est un expert en gestion des crises et des enjeux sensibles.
Ingénieur CESI, il a fondé HEIDERICH il y a 25 ans, une entreprise pionnière en conseil et formation, intervenant en Europe, Afrique et au Brésil sur des situations de crise.
Président de l'Observatoire International des Crises, il a co-inventé le concept de communication sensible et conduit des travaux sur la gestion des incertitudes, les crises cyber, la désinformation et la prise de décision complexe.
Conférencier à l'INSP, l'IHEDN et l'ENM, Didier est également l'auteur de plusieurs ouvrages, dont "Plan de gestion de crise", publié chez Dunod.
www.heiderich.fr

À LIRE

DU MÊME AUTEUR ...

Nokia, un cas d'école

L'histoire de Nokia est un exemple frappant de l'importance d'une gestion proactive des enjeux sensibles pour renforcer la résilience des organisations. La résilience, rappelons-le, n'est pas une méthode, mais un état à cultiver pour mieux affronter les turbulences.

Transition vers les smartphones

Face à l'émergence des smartphones, notamment l'iPhone et les appareils Android, Nokia, alors leader des téléphones mobiles, a sous-estimé l'ampleur du changement. L'entreprise n'a pas su répondre aux attentes des consommateurs, qui privilégiaient des appareils multifonctionnels et innovants.

Innovation et R&D

Malgré des investissements massifs en recherche et développement, Nokia n'a pas produit d'innovations suffisamment disruptives pour rivaliser avec les nouveaux acteurs. L'intégration et la commercialisation des nouvelles technologies étaient trop lentes pour suivre le rythme du marché.

Gestion proactive des enjeux sensibles

Une approche proactive aurait permis à Nokia de mieux intégrer les nouvelles technologies et d'accélérer ses cycles d'innovation. La collaboration avec des startups et une organisation plus agile auraient renforcé sa capacité à rester compétitive.

Culture et gestion du changement

La culture interne de Nokia, bien que forte, manquait de flexibilité face aux transformations. La lenteur des processus décisionnels et une certaine rigidité organisationnelle ont limité sa capacité d'adaptation.

Leçon clé

Pour maintenir sa position, Nokia aurait dû promouvoir une culture d'agilité, réduire la bureaucratie et favoriser l'expérimentation. Une telle stratégie aurait permis une meilleure anticipation des tendances et une adaptation rapide aux opportunités émergentes, éléments essentiels pour la résilience d'une organisation.

FORMATION

Leadership en période de crise

15 au 16 mai 2025

Québec 8h à 12h | France 14h à 18h

FORMATION EN DIRECT VIA TEAMS

Transformez le chaos en opportunité

Inscrivez-vous dès maintenant pour garantir votre place !

Profitez de notre ...

GARANTIE SATISFAIT OU REMBOURSÉ*

👉www.academiecriseetresilience.com/leadership-en-periode-de-crise

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

Les enjeux liés à la gestion de crise cyber en contexte hybride

De nos jours, subir une crise, notamment cyber, est un risque fort de tous types d'entreprises.

La gestion de celle-ci est un enjeu déterminant pour le top management (ou direction générale), mais rares sont les sociétés qui peuvent espérer mobiliser l'ensemble des acteurs de crise dans une même pièce au même moment.

Adrian Vallecchia

Cybersecurity Team Leader & Group Crisis Manager (ou chef d'équipe en cybersécurité et gestionnaire d'un groupe de gestion de crise. chez ALTEN

À l'ère de la digitalisation et de l'accroissement frénétique des possibilités technologiques, faire face à une crise cyber est loin d'être une partie de plaisir.

Dans ce contexte spécifique, il apparaît pertinent de soulever et d'approfondir les défis qui pèsent sur une organisation de crise en mode hybride (présentiel/distanciel).

Soyons honnêtes, à part très peu de contextes bien spécifiques, nous nous dirigeons vers des gestions de crises bien plus orientées sur l'hybride que sur le présentiel.

J'entends par là qu'il y a fort à parier que l'ensemble des parties prenantes clés impliquées dans votre cellule de crise ne soient pas capables d'être toutes présentes physiquement, pour des raisons variées :

- Congé et voyage;
- Business trip (ou voyages d'affaires) en cours ou salon professionnel;
- Cellule de crise trop distante (salarié expatrié, travaille depuis une autre ville);
- Indisponibilité totale.

Partons donc du postulat, réaliste, qu'une partie des acteurs clés pourra simplement participer à la crise à distance.

Cela va sans dire que le fait de mixer des personnes à la fois à distance et en présentiel impose un défi majeur au directeur de crise, qui devra trouver un équilibre concernant plusieurs aspects :

- La gestion de la communication entre les acteurs de la cellule de crise et en dehors de celle-ci;
- La gestion de la transition de l'information pendant la crise (réussir à garder un niveau d'information homogène afin de garder un rythme cohérent);
- La gestion du stress potentiel des acteurs impliqués;
- La gestion technique des outils utilisés pour communiquer (problèmes techniques divers liés aux applicatifs utilisés, ou simplement de connexion/réseau liés à l'acteur de crise);
- La gestion des échanges rapides entre les équipes autour de la remédiation technique et stratégique (allant du forensique jusqu'au *recovery* (ou reprise), en passant par l'analyse des impacts business et légaux).

Une des clés d'une gestion de crise réussie est, selon moi, notre capacité à gagner du temps ou plutôt à économiser du temps (au-delà des aspects business, cela peut grandement faciliter la remédiation technique en cas de crise cyber, par exemple).

L'efficience est, je pense, ce à quoi il faut tendre lorsqu'on s'attache à créer un processus de gestion de crise de qualité qui fonctionne.

Afin de répondre de façon pragmatique à ces défis, il existe des actions/options à mettre en place afin de maximiser la capacité de coordination et de travail une fois que la cellule de crise est mobilisée :

- Mettre en place et rappeler, durant le briefing initial, les règles dédiées à la gestion de crise hybride.
- Prévoir des outils de communication fiables et résilients.
- Prévoir des backups (alternatives) de ces outils et, idéalement, implémenter un outil de gestion de crise (Everbridge, Cedralis, F24…) qui permet de donner de la profondeur à ses capacités opérationnelles, notamment en cas de perte du SI.
- Tester régulièrement les outils à travers des exercices dédiés.
- Prévoir un chapitre (ou plus au besoin) dans la documentation spécifique pour les acteurs distanciels.
- Inclure ces aspects dans les entraînements (obliger des acteurs en présentiel à faire l'exercice à distance afin de se rendre compte des enjeux, par exemple) et les sensibilisations en place chaque année.
- Former et sensibiliser le directeur de crise à ces aspects en amont ainsi que les acteurs clés de la crise.
- Identifier en amont, dans l'annuaire de crise, les acteurs clés distanciels (si possible).
- Tenir une main courante ainsi qu'un plan de remédiation visibles et accessibles à tous afin de fluidifier les actions ainsi que le partage d'informations.
- Toujours considérer les défis de l'hybride durant chaque retour d'expérience (RETEX) postcrise afin de toujours proposer une démarche d'amélioration continue (PDCA).

Globalement, un des atouts de votre équipe de crise sera toujours sa capacité à se connaître et à bien envisager ses forces et ses faiblesses.

Attention, l'objectif ici n'est pas d'expliquer que la gestion de crise en mode hybride est une faiblesse; au contraire, elle peut être très pertinente. Nous avançons ici que la gestion de crise en elle-même est déjà complexe et que l'ajout de modalités hybrides implique une connaissance des enjeux ainsi que des actions à mettre en place afin de rendre l'ensemble efficient.

À l'inverse, sans préparation et anticipation de ces aspects hybrides, il est fort probable que l'on perde beaucoup de temps à tenter de trouver un équilibre pendant la crise.

Finalement, comme souvent en gestion de crise, il est question de préparation, de structuration et d'anticipation de ces enjeux.

La mise en place d'une documentation suivant des standards solides couplée avec une équipe formée et sensibilisée saura canaliser les défis d'une gestion de crise hybride.

Il y aura perpétuellement des imprévus ainsi que des dysfonctionnements le moment venu. Il est question ici de savoir anticiper tout ce qui est préparable.

« Les tuiles qui nous protègent de la pluie ont toutes été posées par beau temps. »

Proverbe chinois

Adrian VALLECCHIA

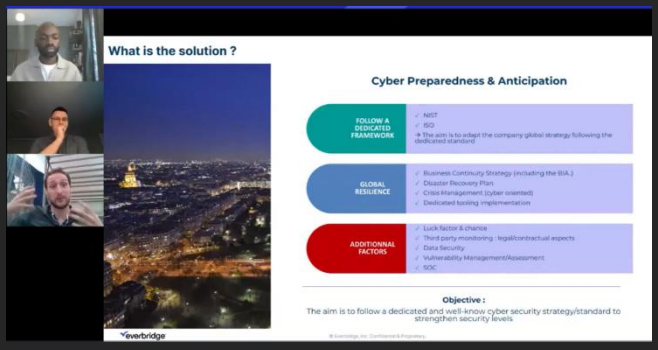
J'occupe des fonctions transversales en tant que Team leader Cybersecurity & Group Crisis Manager pour le compte de la DSI du groupe ALTEN, dans les équipes du RSSI opérationnel, depuis Singapour (2022).

Spécialisé en cybersécurité GRC (gouvernance, risques, conformité) axée sur la crise cyber.

https://www.alten.fr/

À VOIR

WEBINAIRE RÉSILIENCE ET CYBERSÉCURITÉ…



Conseils pour rendre plus efficiente une gestion de crise hybride

Une crise hybride implique que les acteurs clés de la crise soient disponibles et capables de travailler à la fois depuis la cellule de crise et à distance.

Dans ce cas bien précis, il est essentiel d'adapter son mode de travail, la capacité de répartition des tâches et de gestion de l'information ainsi que le contrôle des événements en cours.

Pour ce faire, voici quelques réflexes et conseils à mettre en place dans un cadre hybride :

- Inclure/prévoir dans la documentation des moyens de communication/gestion efficaces et sécurisés permettant d'avoir tout le monde sur le pont (voir outils conseillés par l'ANSSI)
- Bonus : privilégier l'implémentation d'un outil (type Everbridge) afin d'augmenter à la fois vos capacités hybrides et votre résilience dans un contexte de crise.
- Favoriser la mise en place de règles spécifiques en cellule dès la mobilisation (briefing initial) afin de bien encadrer la communication et les temps de parole (ex. : point de situation).
- Toujours garder à l'esprit que les personnes à distance font partie intégrante de la crise (tendance à plus considérer les personnes présentes physiquement).
- Fait toujours signer un NDA (non-disclosure agreement ou, en français, accord de non-divulgation) à l'ensemble des personnes entrant en cellule de crise. La gestion hybride demande une capacité de communication accrue et un besoin de protéger/cloisonner l'information sensible parmi les acteurs habilités.
- Tenir une main courante ainsi qu'un plan de remédiation visibles et accessibles à tous afin de fluidifier les actions ainsi que le partage d'informations.
- Rappeler que toutes les informations utiles doivent être communiquées aux bons acteurs (log keepers/crisis coordinators) afin qu'elles figurent dans la main courante. Les actions doivent l'être dans le plan de remédiation.

FORMATION

Élaborez un exercice de gestion de crise

26 au 29 mai 2025

Québec 8h à 12h | France 14h à 18h

FORMATION EN DIRECT VIA TEAMS

De l'idée à l'action : créez votre exercice de gestion de crise, étape par étape !

Inscrivez-vous dès maintenant pour garantir votre place !

Profitez de notre ...

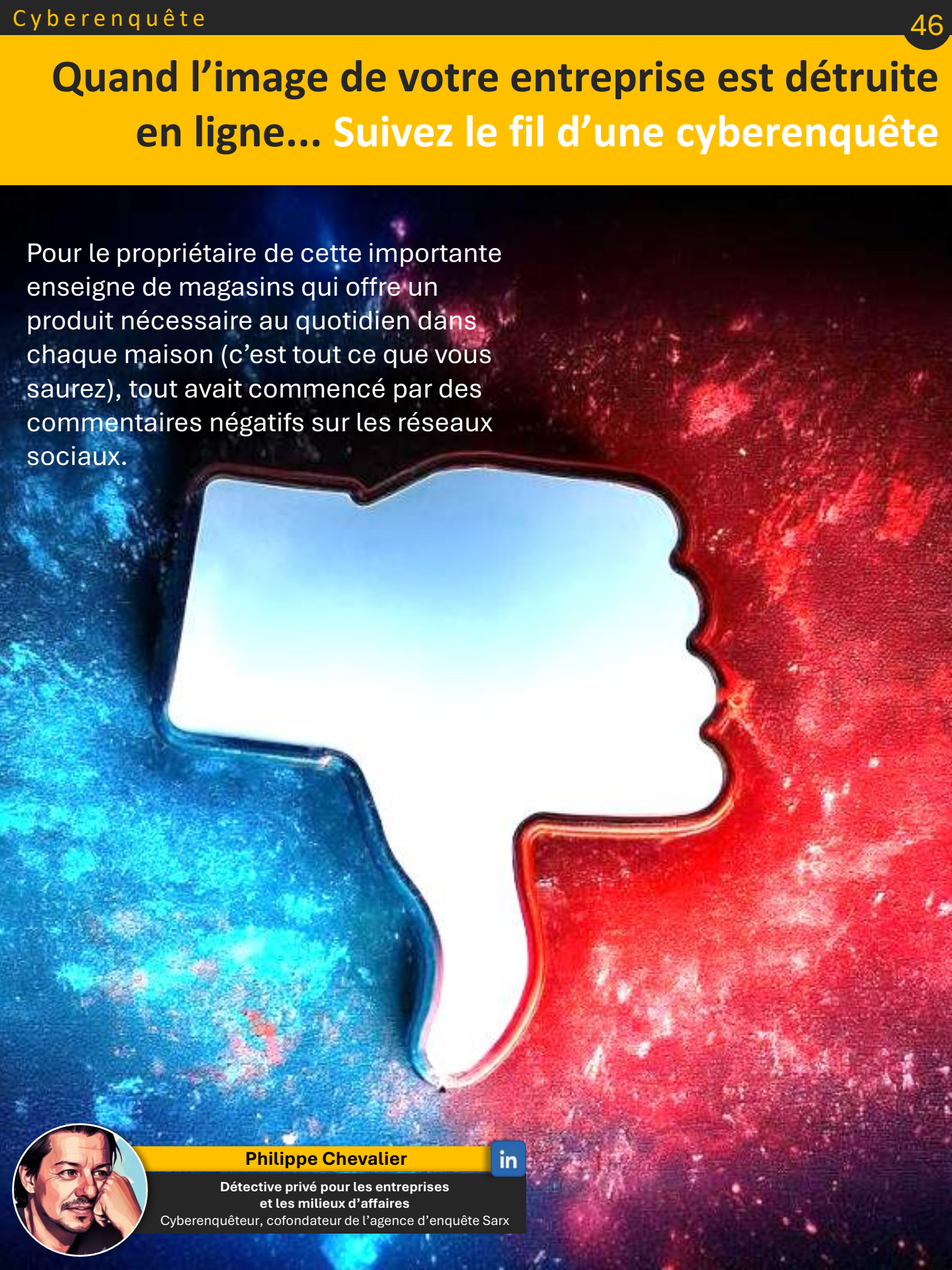
GARANTIE SATISFAIT OU REMBOURSÉ.*

👉www.academiecriseetresilience.com/elaborez-exercice-de-crise

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

Quand l’image de votre entreprise est détruite en ligne... Suivez le fil d’une cyberenquête

Pour le propriétaire de cette importante enseigne de magasins qui offre un produit nécessaire au quotidien dans chaque maison (c’est tout ce que vous saurez), tout avait commencé par des commentaires négatifs sur les réseaux sociaux.



Philippe Chevalier

Détective privé pour les entreprises et les milieux d’affaires

Cyberenquêteur, cofondateur de l’agence d’enquête Sarx

Rapidement, en quelques semaines, tout s'était accéléré : les avis Google, les avis sur les sites de consommateurs, les posts et commentaires sur LinkedIn (cela est plus surprenant), jusqu'au coup final : un appel d'un journaliste de Québecor.

L'entreprise s'était pourtant forgé une belle réputation au fil des années. Elle était même sur le point de voir son nom devenir synonyme du produit : comme Frigidaire pour les réfrigérateurs, ou Bikini pour les costumes de bain deux-pièces dans les années 1930.

Mais, là... Tout semblait compromettre brutalement la réputation de l'entreprise : la qualité des produits était attaquée, de même que la qualité du service. L'entreprise ne comprenait pas ce qui se passait :

> Admettons qu'il y ait quelques clients insatisfaits, comment est-ce possible en quelques semaines, alors que le produit et le service n'ont pas changé?
>
> Admettons que quelques clients deviennent des fanatiques acharnés n'ayant pas d'autres loisirs que de blaster ou torpiller la marque sur les réseaux sociaux, mais comment se seraient-ils coordonnés?
>
> Admettons que cela vienne d'un compétiteur déloyal, comment peut-il disposer d'une telle force de frappe sur tous les réseaux sociaux? Jusqu'à aller chercher de grands médias?
>
> Admettons que cela vienne d'un employé congédié, comment trouve-t-il les moyens techniques et financiers de mettre en œuvre une campagne de dénigrement?

Toutes ces questions sont autant d'hypothèses pour une agence de cyberenquête, autant de portes à ouvrir et à refermer au fur et à mesure que les doutes sont levés ou confirmés.

Alors, commençons :

- Les clients insatisfaits n'agissent pas en commando, mais, éventuellement, ils se regroupent sur un site dédié, ou une page dédiée. Certains sont des quérulents, c'est-à-dire des personnes dont la passion (le loisir) est de multiplier les plaintes. Les tribunaux ont fini par se lasser et les personnes déclarées quérulentes par la Cour du Québec sont inscrites à un fichier public. Ici, rien de tout cela.

Notez qu'il est possible d'acheter en Inde des avis négatifs par paquet de 500 pour 2 $ l'avis à partir de vrais profils et de vrais comptes Google. Mais ce n'est pas le cas dans cette affaire.

Notez également qu'il existe des groupes Facebook où des Québécois authentiques vendent leurs avis négatifs ou positifs sur n'importe quelle entreprise à votre demande. Mais rien de cela dans notre affaire.

- L’entreprise n’a pas de compétiteurs sur son marché, sauf des artisans, ou des manufacturiers, qui visent un autre public. L’entreprise visée offre un produit unique qui plaît ou ne plaît pas, mais aucun compétiteur ne la dérange. Cette hypothèse est refermée.

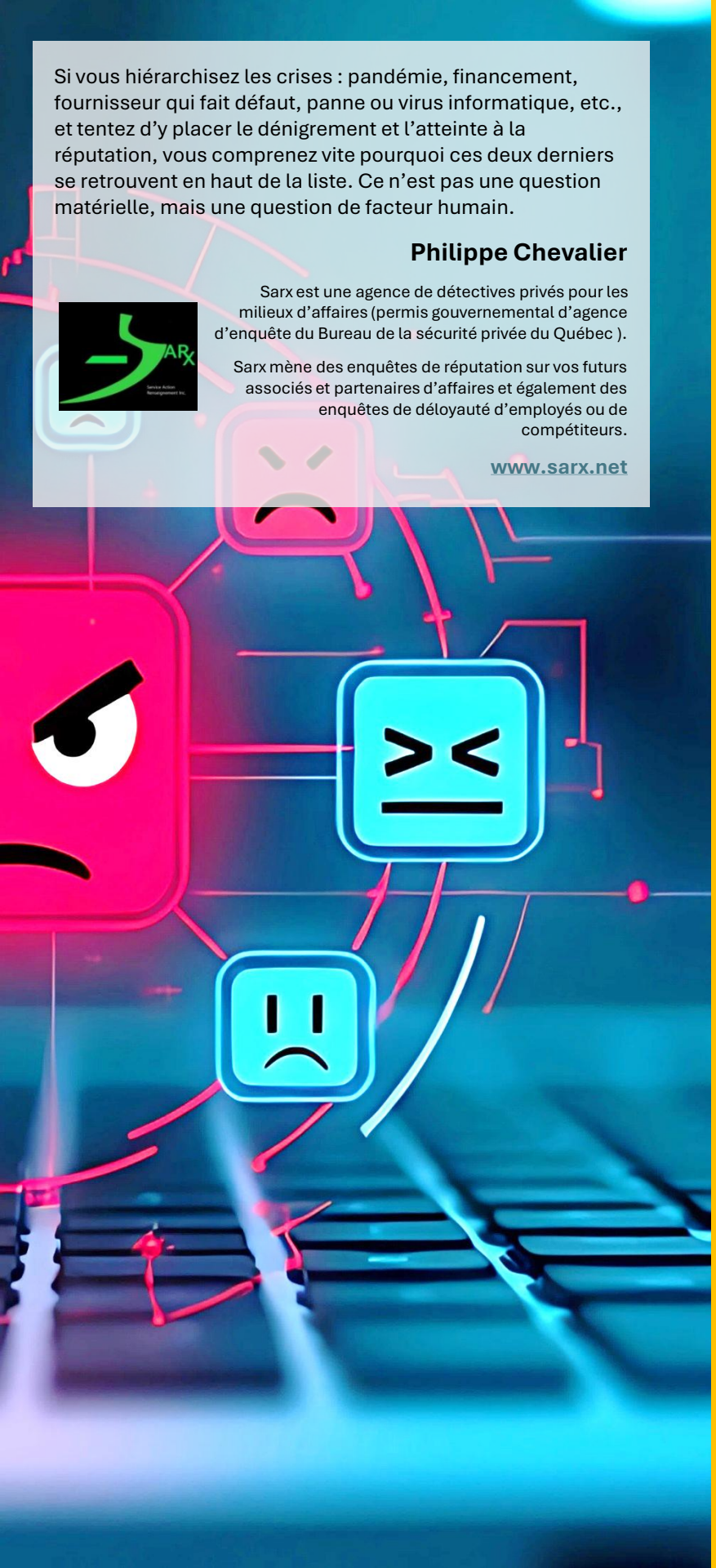
Notez cependant que le dénigrement organisé par un compétiteur est très fréquent dans les secteurs suivants : hôtellerie, restauration, construction, rénovation, franchises alimentaires ou de produits, animaleries, cliniques esthétiques, tourisme, transport aérien, concessions auto, etc.

- Un employé fâché et congédié? Là… il y a quelque chose! Sachez que là se trouve la puissance des émotions, de la vraie colère, de l’irrationnel et même de la haine obsessionnelle, peut-être même dangereuse! Alors oui, nous avions procédé à de la triangulation de données et créé une cartographie des adresses courriel agressives. Les liens étaient clairs et surtout démontrés. Tout remontait à un point de départ unique.

De plus, un profil LinkedIn parmi ceux des employés ayant récemment quitté l’entreprise était intrigant : des commentaires déçus, en colère contre le marché du travail, pas de nouvel emploi, et un style de rédaction (choix des mots, ponctuation, structure) très semblable aux messages de dénigrement. De même, cet individu était passionné par les pages de commentaires du Journal de Montréal, où il était actif… Mais cela ne donne pas de preuves. La preuve fut établie par des moyens électroniques (en source ouverte) et une conversation sous de faux motifs, mais sans pièges, en incitant la cible à s’exprimer et à assumer ses dires.

Résultat : après sept jours d’enquête, il fut possible d’amener des preuves. L’entreprise a préféré négocier (la majorité des cas se finissent en négo et non pas devant un tribunal) et le harcèlement numérique s’est arrêté; puis, rétroaction de l’harceleur et retrait des commentaires, communication avec le journaliste qui renonce, bref… fin des hostilités. Cela dit… Ce qui vous intéresse, c’est la résilience après crise, mais cette résilience passe par une étape préalable. Pas de déni : le dénigrement en ligne, organisé par des clients, des concurrents, des ex-associés ou des ex-employés, cela arrive à toute entreprise.

Quant aux anciens employés et aux ex-associés qui vous attaqueraient, c’est une autre dimension. Elle se prouve par une cyberenquête, sans attendre, car l’atteinte à la réputation de votre entreprise de la part de personnes malveillantes, c’est l’événement le plus lourd qui puisse arriver à une entreprise.



Si vous hiérarchisez les crises : pandémie, financement, fournisseur qui fait défaut, panne ou virus informatique, etc., et tentez d'y placer le dénigrement et l'atteinte à la réputation, vous comprenez vite pourquoi ces deux derniers se retrouvent en haut de la liste. Ce n'est pas une question matérielle, mais une question de facteur humain.

Philippe Chevalier

Sarx est une agence de détectives privés pour les milieux d'affaires (permis gouvernemental d'agence d'enquête du Bureau de la sécurité privée du Québec).

Sarx mène des enquêtes de réputation sur vos futurs associés et partenaires d'affaires et également des enquêtes de déloyauté d'employés ou de compétiteurs.

www.sarx.net

Surmonter et contre-attaquer

Cela n'arrive pas qu'aux autres.

- Acceptez l'idée que la mauvaise foi fait partie de l'environnement normal des affaires, même si des clients peuvent donner.
- Surveillez la concordance de style et de dates des rumeurs négatives ainsi que des attaques en ligne.
- Pensez aux trois causes possibles : client; concurrent; ex-employé et ex-associé.
- Observez ce qui serait logique pour chacune de ces origines.
- Donc, pensez comme l'adversaire pour mieux appréhender la cause du problème.
- Parmi ces trois ressources extérieures, chacune a son utilité précise :
    - Avocat pour définir et mettre en œuvre vos moyens d'action;
    - Relationniste de crise pour faire face;
    - Cyberenquêteur (avec permis d'agence d'enquête) pour prouver ou documenter.

Pour optimiser ces ressources et ne pas vous ruiner, l'avocat doit vous accompagner une fois que des éléments de preuve sont réunis pour une plainte ou une négociation.

Le relationniste doit être expérimenté en relations médias (médias traditionnels et médias sociaux). Il ne va pas gérer votre défense, mais vous dire comment procéder.

Le cyberenquêteur doit être familier avec les milieux d'affaires et les méthodes agressives de vos adversaires. Il doit être à la fois un détective d'affaires autorisé et un hacker. Les conclusions de son rapport doivent être sourcées, démontrées, prouvées. Car votre avocat ou vous-même devrez disposer d'éléments concrets.

Quand le loup... est dans la bergerie

Dans le monde de la cybersécurité, on s'attend souvent à ce que les menaces viennent de l'extérieur.

Pourtant, l'affaire récente qui a secoué le secteur de la santé en Bretagne et dans les Pays de la Loire nous rappelle que parfois, le danger se cache au cœur même de nos institutions.

Tel un loup déguisé en berger, un ancien responsable de la sécurité informatique a orchestré une attaque dévastatrice contre son ancien employeur, mettant en péril la santé et la sécurité de nombreux patients.

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.

Le Groupe Hospitalier Grand Ouest (GHGO), gestionnaire de neuf établissements de santé dans ces régions, a été frappé par une cyberattaque d'une ampleur sans précédent entre le 2 et le 4 octobre 2024.

Cette attaque, initialement identifiée comme une attaque DDoS (Distributed Denial of Service), visait à paralyser les systèmes d'information vitaux de ces établissements. La clinique mutualiste La Sagesse à Rennes a été particulièrement touchée, contrainte de reporter plusieurs interventions chirurgicales, mettant ainsi en danger la vie de patients en attente de soins urgents.

Ce qui semblait être une attaque classique de cybercriminels a pris une tournure inattendue lorsque les attaquants ont exigé une rançon de 650 741 dollars pour débloquer le système.

Cette demande, inhabituelle pour une attaque DDoS, a éveillé les soupçons des enquêteurs du Centre de lutte contre les criminalités numériques (C3N) de l'Unité nationale cyber (UNC). Leur intuition les a conduits sur une piste surprenante : et si le loup se cachait parmi les agneaux ?

L'enquête minutieuse menée par le C3N et son antenne rennaise a rapidement révélé des indices de compromission interne.

Le 17 décembre, les autorités ont arrêté un suspect inattendu : un ancien responsable de la sécurité informatique du GHGO, âgé de seulement 26 ans.

Ce jeune homme, qui avait occupé le poste d'administrateur réseau depuis juillet 2024 avant de démissionner en octobre de la même année, était censé être le gardien des systèmes qu'il a finalement attaqués.

Le modus operandi du suspect ajoute une couche de complexité à l'affaire.

En envoyant des mails de menace en anglais et en russe au personnel des établissements, il a tenté de brouiller les pistes, se faisant passer pour un groupe de cybercriminels internationaux.

Cette tactique souligne la sophistication croissante des menaces internes et la nécessité d'une vigilance accrue, même envers ceux en qui nous plaçons notre confiance.

Les conséquences de cette trahison vont bien au-delà des dommages immédiats causés aux systèmes informatiques.

Cette affaire soulève des questions troublantes sur la sécurité interne de nos organisations.

- Comment un individu censé protéger ces systèmes critiques a-t-il pu se retourner contre eux ?
- Quelles failles dans les procédures de sécurité ont permis à cet ancien employé de conserver un accès aussi destructeur après son départ ?

Elle ébranle la confiance que les patients et le personnel médical placent dans la sécurité de leurs données et de leurs infrastructures critiques.

Comment les établissements de santé peuvent-ils garantir la confidentialité et l'intégrité de leurs systèmes face à des menaces venant de l'intérieur ?

Le suspect comparaîtra devant le tribunal le 6 février prochain pour répondre des charges d' *"entrave à un système de traitement automatisé de données"* et de *"suppression et extraction de données"*.

Mais au-delà de la procédure judiciaire, cette affaire doit servir de signal d'alarme pour toutes les organisations.

Il est crucial que les organisations renforcent non seulement leurs défenses contre les menaces externes, mais aussi leurs protocoles de sécurité interne. Cela implique une gestion plus rigoureuse des accès, des audits réguliers des systèmes, et une surveillance accrue des activités suspectes, y compris celles des employés de confiance.

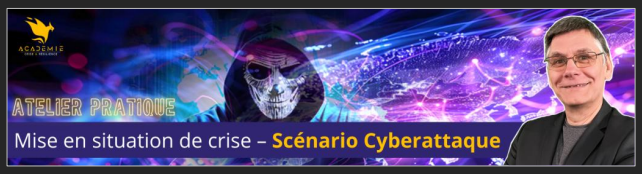
Cette affaire nous rappelle que dans le monde numérique, comme dans la fable du loup et de l'agneau, la vigilance doit être constante. Car parfois, le plus grand danger ne vient pas de l'extérieur, mais de celui qui était censé nous protéger.

Alexandre Fournier

Consultant et formateur expert en continuité des affaires et gestion de crise. J'accompagne depuis plus de 30 ans, les organisations pour développer leur résilience face aux perturbations majeures.

https://www.linkedin.com/in/alexandre-fournier-1363125/

Inscrivez-vous à cet exercice!



Académie **Crise & Résilience**

FORMATION

Intégrez l'IA dans la Gestion de Crise

18-19 février 2025

Québec 8h à 12h | France 14h à 18h

FORMATION EN DIRECT VIA TEAMS

L'IA à vos côtés avant, pendant et après la crise!

Inscrivez-vous dès maintenant pour garantir votre place !

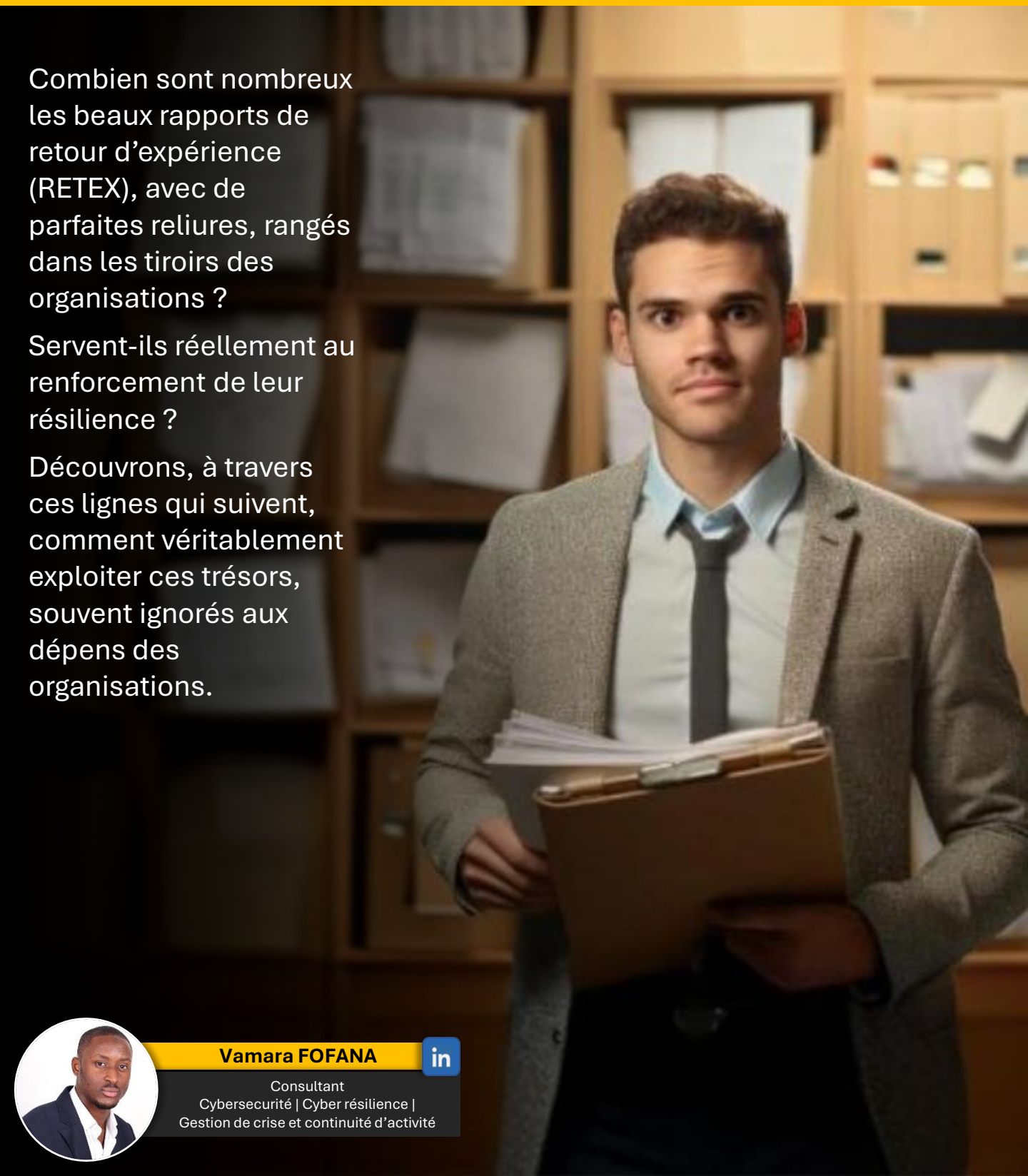
Profitez de notre ...

GARANTIE SATISFAIT OU REMBOURSÉ*

👉www.academiecriseetresilience.com/integrer-ia-et-gestion-de-crise

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

Quelle gouvernance pour capitaliser réellement sur un retour d'expérience post-crise ?



Combien sont nombreux les beaux rapports de retour d'expérience (RETEX), avec de parfaites reliures, rangés dans les tiroirs des organisations ?

Servent-ils réellement au renforcement de leur résilience ?

Découvrons, à travers ces lignes qui suivent, comment véritablement exploiter ces trésors, souvent ignorés aux dépens des organisations.

Vamara FOFANA

Consultant
Cybersecurité | Cyber résilience |
Gestion de crise et continuité d'activité

Le risque zéro n'existe pas. Les crises sont donc inéluctables. Les organisations doivent ainsi se focaliser sur la gestion de leur occurrence, mais surtout sur la capitalisation des leçons apprises qui en découlent.

Cet article explore la gouvernance nécessaire pour exploiter efficacement les retours d'expérience (RETEX) et renforcer ainsi la résilience organisationnelle.

Le RETEX, une étape nécessaire

Le retour d'expérience consiste à analyser les actions réalisées (ou non réalisées) en situation de crise (réelle ou simulée) qu'elles soient positives ou négatives.

Le but ultime ? En tirer des enseignements concrets permettant d'être plus résilients.

Plus pratiquement, cela peut consister à se poser, sans biais cognitifs, un certain nombre de questions concrètes, sous différents formats (questionnaire, entretiens, plénière, etc.), parmi lesquelles :

- Est-ce que les signaux faibles ont été considérés ?
- Quels ont été les délais de réponse ?
- Aurions-nous fait mieux ?
- L'organisation de la salle de crise était-elle ergonomique ?
- Les plans de résilience (plan de gestion de crise, plan de continuité des activités) étaient-ils cohérents/utiles ?

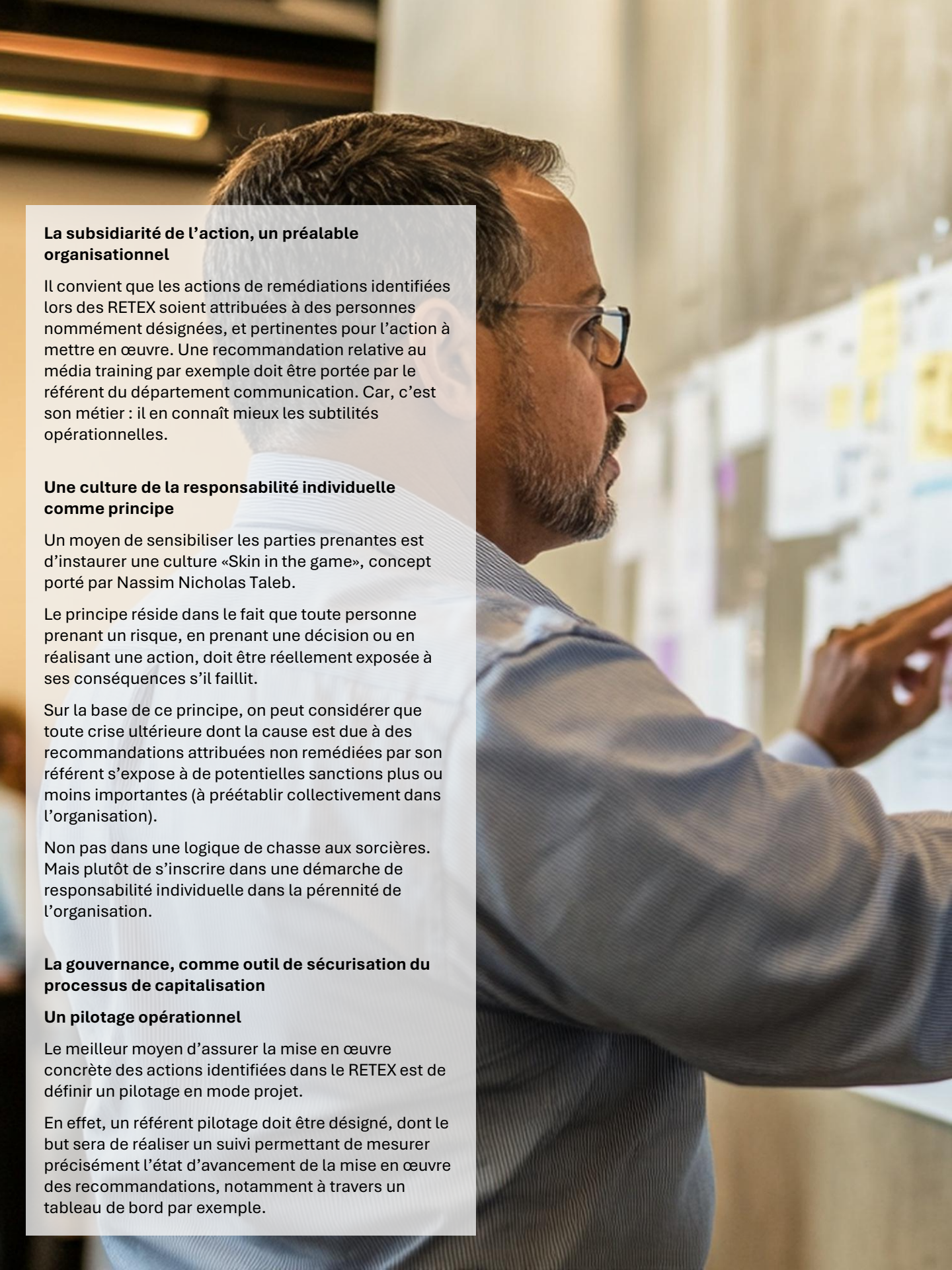
Bref, la liste n'est bien entendu pas exhaustive.

La réponse à ces interrogations permettra d'une part d'identifier les mécanismes organisationnels et humains ayant fonctionné et les dysfonctionnements. D'autre part, cela doit donner lieu à des axes d'amélioration du dispositif de résilience sur le plan organisationnel, humain et logistique.

Est-ce suffisant ?

Malheureusement, les RETEX se réduisent quelquefois à de beaux rapports rangés aux tiroirs. Or, l'essence même de la capitalisation réside dans l'exploitation opérationnelle des axes d'amélioration.

Sans gouvernance structurée, le RETEX n'est qu'une case cochée pour se rassurer que le travail soit fait, en attendant l'occurrence d'une nouvelle crise.



La subsidiarité de l'action, un préalable organisationnel

Il convient que les actions de remédiations identifiées lors des RETEX soient attribuées à des personnes nommément désignées, et pertinentes pour l'action à mettre en œuvre. Une recommandation relative au média training par exemple doit être portée par le référent du département communication. Car, c'est son métier : il en connaît mieux les subtilités opérationnelles.

Une culture de la responsabilité individuelle comme principe

Un moyen de sensibiliser les parties prenantes est d'instaurer une culture «Skin in the game», concept porté par Nassim Nicholas Taleb.

Le principe réside dans le fait que toute personne prenant un risque, en prenant une décision ou en réalisant une action, doit être réellement exposée à ses conséquences s'il faillit.

Sur la base de ce principe, on peut considérer que toute crise ultérieure dont la cause est due à des recommandations attribuées non remédiées par son référent s'expose à de potentielles sanctions plus ou moins importantes (à préétablir collectivement dans l'organisation).

Non pas dans une logique de chasse aux sorcières. Mais plutôt de s'inscrire dans une démarche de responsabilité individuelle dans la pérennité de l'organisation.

La gouvernance, comme outil de sécurisation du processus de capitalisation

Un pilotage opérationnel

Le meilleur moyen d'assurer la mise en œuvre concrète des actions identifiées dans le RETEX est de définir un pilotage en mode projet.

En effet, un référent pilotage doit être désigné, dont le but sera de réaliser un suivi permettant de mesurer précisément l'état d'avancement de la mise en œuvre des recommandations, notamment à travers un tableau de bord par exemple.

Une comitologie dédiée[1]

Quel intérêt ?

Le compte rendu n'est pas neutre du moment où il doit se faire dans le cadre d'une instance, composée en particulier de représentants du Top management, du responsable de continuité des activités (et du Crisis manager (ou gestionnaire de crise) si distinct), des représentants des départements Risque et Conformité.

Il ne s'agirait pas de communiquer seulement l'état d'avancement de la capitalisation, mais également les points d'attention (non-respect des délais, difficultés techniques, organisationnelles ou budgétaires, etc.).

En outre, chaque réunion doit faire l'objet d'un arbitrage dudit Top management, des avis de la compliance (avis en cas de risque de non-conformité réglementaire par exemple), et du risque (avis sur l'alignement avec le niveau de tolérance au risque de l'organisation).

Les décisions actées doivent nécessairement être traçables et actionnables.

On s'arrête là ? Eh bien... Non sans un "crash test"

Il convient cependant de noter que ces actions sont une condition nécessaire, mais pas suffisante, si les actions mises en œuvre ne sont pas systématiquement mises à rude épreuve.

En effet, **une opération test est indispensable** pour revisiter la solidité des cicatrices de l'organisation.

Avec le même scénario ?

Surtout pas. Le test doit être idéalement réalisé, sans avertir les principaux acteurs de la gestion crise (sur une plage horaire convenable) avec un scénario différent du précédent pour éviter tout biais. Mais avec des objectifs similaires.

Enfin, il convient de reconnaître que la résilience est un idéal plus ou moins atteignable. Les organisations ont à minima une obligation de moyens, en ne laissant la place qu'à l'inéluctable. Absolument rien au hasard.

C'est pourquoi chaque crise doit permettre de grandir davantage, par l'intégration réelle des leçons afférentes.

Pour finir, l'exercice descriptif et normatif des RETEX est essentiel pour renforcer la résilience organisationnelle.

Sans une gouvernance structurée, ces enseignements risquent de rester lettre morte et d'ouvrir la voie à des crises évitables.

Ne limitez pas vos RETEX à des rapports : appliquez les axes d'amélioration, retestez-les, et transformez-les en leviers durables pour anticiper et mieux gérer les crises futures. Elles viendront, soyez-en certains !

Vamara FOFANA

Vamara est Consultant en Cybersécurité/Résilience chez EY (Paris). Ancien membre du centre de crise du ministère de la Santé pendant la COVID-19, il est titulaire de deux Masters : Économie de la Santé (Paris Dauphine) et Gestion des Risques et des Crises (Paris 1 - Sorbonne).

https://www.linkedin.com/in/vamara-fofana-215097147/

5 actions structurantes pour tirer réellement parti de vos RETEX

1. **Désigner des "remediation owners"**: Chaque recommandation formulée doit avoir un responsable spécifique. Ces "remediation owners" doivent être nommément désignés et clairement communiqués à toutes les parties prenantes (acteurs de la crise à minima), garantissant ainsi une responsabilité directe et un suivi rigoureux de la mise en œuvre des actions.

2. **Désigner un référent de pilotage**: Le référent de pilotage doit être identifié afin de superviser la mise en œuvre concrète des recommandations issues des RETEX. Il doit s'assurer que les actions sont réalisées dans les délais impartis.

3. **Mettre en place une comitologie**: Une comitologie, incluant la direction, le responsable de la conformité, le responsable du risque, et d'autres parties prenantes pertinentes le cas échéant, doit être mise en place pour suivre l'avancement des actions, évaluer les risques associés et faciliter la prise de décision stratégique.

4. **Tester le dispositif actualisé**: Il est essentiel de tester régulièrement le dispositif mis à jour à travers des simulations surprises basées sur des scénarios variés. Ces tests doivent permettre de vérifier la réactivité des parties prenantes, l'efficacité des recommandations et d'identifier des axes d'amélioration complémentaires le cas échéant.

5. **Améliorer en continu du processus de capitalisation**: L'organisation doit inscrire la gestion des RETEX de bout en bout dans une démarche d'amélioration continue, en révisant régulièrement leur pertinence. Revisitant les crises passées, elle peut ajuster les priorités et renforcer sa capacité d'anticipation pour mieux gérer les crises futures.

Événements a venir

FORMATION

Mettre en place un Plan de reprise informatique

7 Ateliers de 3h
du 13 mars au 1 mai 2025
Québec 13h à 16h - EN DIRECT VIA TEAMS

Réagissez vite, réagissez bien: bâtissez un plan de reprise informatique bien pensé!

Inscrivez-vous dès maintenant pour garantir votre place !

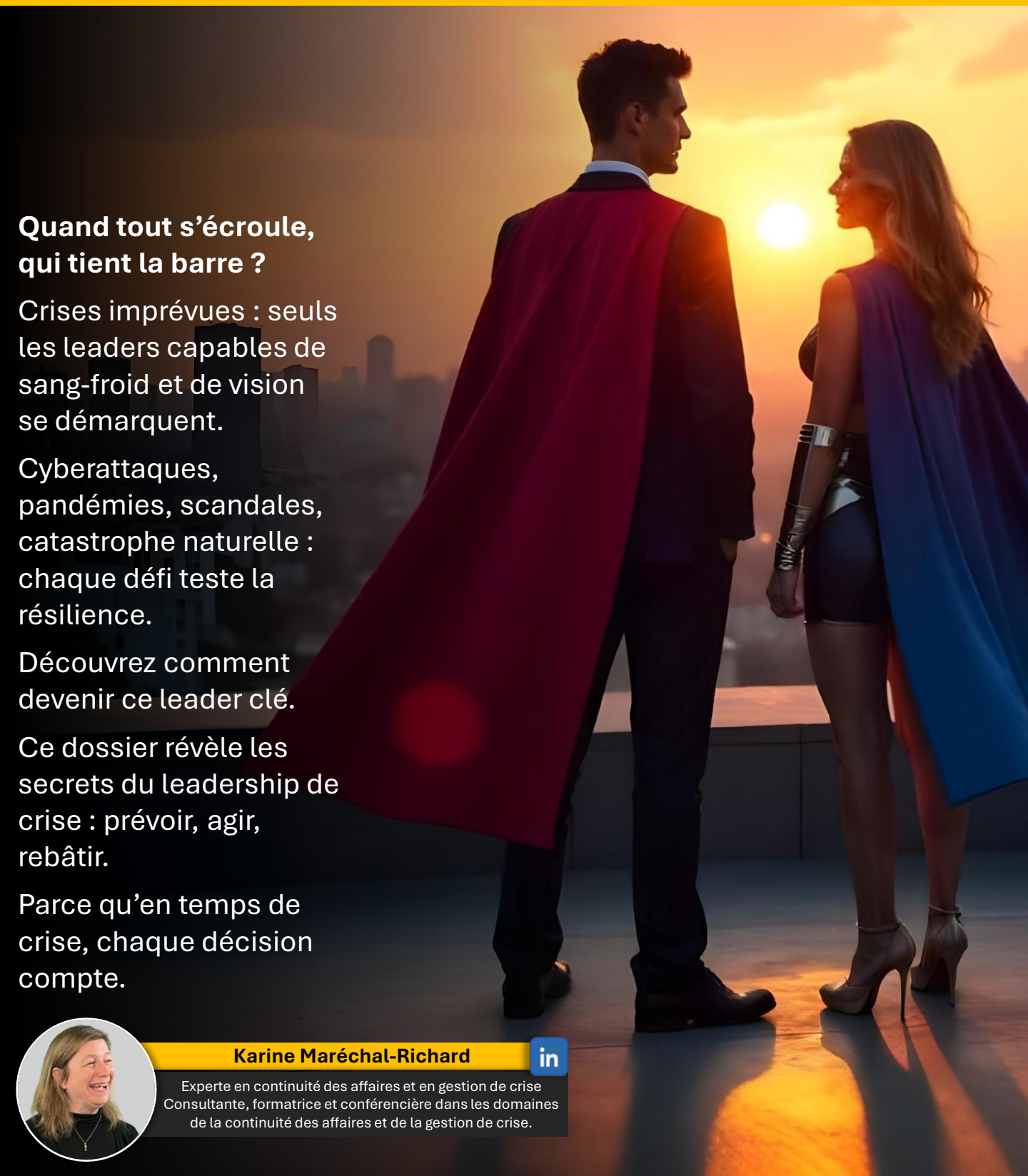
Profitez de notre ...

GARANTIE SATISFAIT OU REMBOURSÉ.*

👉www.academiecriseetresilience.com/plan-de-reprise-informatique

*Si au bout de 90 minutes, vous vous apercevez que cette formation n'est pas pour vous, nous vous la remboursons !

Leadership en période de crise
Transformez le chaos en opportunité



Quand tout s'écroule, qui tient la barre ?

Crises imprévues : seuls les leaders capables de sang-froid et de vision se démarquent.

Cyberattaques, pandémies, scandales, catastrophe naturelle : chaque défi teste la résilience.

Découvrez comment devenir ce leader clé.

Ce dossier révèle les secrets du leadership de crise : prévoir, agir, rebâtir.

Parce qu'en temps de crise, chaque décision compte.

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.

Dans un monde où les imprévus et les changements rapides sont la norme, le leadership de crise s'impose comme une compétence essentielle. Les crises prennent des formes variées : cyberattaques paralysant des systèmes entiers, pandémies mondiales, crises économiques dévastatrices, scandales médiatiques compromettants ou catastrophes naturelles bouleversantes.

Dans ces moments critiques, les leaders jouent un rôle central : ils guident leurs équipes et leurs organisations à travers des turbulences imprévisibles.

Pourquoi les crises révèlent-elles les véritables leaders ? Parce qu'elles exigent d'eux sang-froid, lucidité et capacité à naviguer dans l'incertitude.

Une crise, par définition, est un mélange de stress, de pression et de chaos. Être leader dans ces conditions, c'est comme piloter un navire en pleine tempête sans carte ni boussole. Seules des qualités exceptionnelles, comme la résilience et une vision stratégique, permettent de transformer ces défis en opportunités.

Mais une crise n'est pas qu'un défi opérationnel. Elle frappe aussi sur le plan émotionnel :

- Les équipes peuvent être paralysées par la peur ou submergées par le stress. Elles ont besoin d'un leader capable de les rassurer et de raviver leur motivation.
- Les dirigeants, quant à eux, font face à des décisions complexes et irréversibles, où l'incertitude domine. Imaginez jouer aux échecs contre la montre, sous une pression constante.

Les défis du leadership en temps de crise

Gérer une crise, c'est comme naviguer dans une tempête avec des outils parfois incomplets ou qui fonctionnes partiellement. Voici les principaux défis que doivent affronter les leaders :

- **L'incertitude :** Vous n'aurez pas toujours toutes les réponses, et il faut apprendre à avancer malgré cela. Accepter l'incertitude est une preuve de maturité et de résilience.
- **Le temps limité :** La rapidité devient souvent plus cruciale que la perfection. Mieux vaut une décision imparfaite mais rapide qu'une solution idéale arrivée trop tard.
- **Le manque de données fiables :** Les leaders doivent s'appuyer sur des informations fragmentaires et faire confiance à leur intuition autant qu'à leurs analyses.

"Le leadership de crise, c'est l'art de transformer le chaos en opportunité de renouveau."

Karine Maréchal-Richard

Dans chaque situation, la capacité d'un leader à prendre des décisions réfléchies, à garder son calme et à rassembler ses équipes autour d'une vision commune peut faire la différence entre échec et succès. Le leadership de crise, c'est l'art de transformer le chaos en opportunité de renouveau.

Qualités essentielles d'un leader de crise[1]

Pour affronter l'imprévisible et inspirer la confiance, un leader de crise doit cultiver des qualités uniques qui le distinguent :

- **Résilience :** Tomber sept fois, se relever huit. La crise n'épargne personne, mais c'est votre capacité à rebondir qui détermine votre réussite.
- **Adaptabilité :** Savoir ajuster les voiles quand le vent change de direction, même en plein vol. La flexibilité est votre boussole dans le chaos.
- **Intelligence émotionnelle :** Rester humain, même sous une pression écrasante. Comprendre et gérer les émotions, les vôtres comme celles des autres, est crucial pour maintenir la cohésion.
- **Communication claire :** Parler comme un GPS précis, sans détour ni jargon. En temps de crise, vos messages doivent être simples, directs et inspirants – pas comme un manuel de micro-ondes impossible à déchiffrer.

Différences entre leadership classique et leadership de crise

Les crises bouleversent les règles du leadership. Ce qui fonctionne en temps normal peut devenir un obstacle en période de turbulence :

- **Planification vs Survie :** En temps normal, vous élaborez des stratégies à long terme. En crise, vous naviguez au jour le jour, cherchant des solutions rapides et pragmatiques.
- **Participation vs Décision rapide :** Le leadership classique valorise la collaboration et la consultation. Mais en temps de crise, vous devez souvent prendre des décisions directes et fermes, parfois seul

Un leader efficace est celui qui sait jongler entre ces deux approches, passant de l'une à l'autre selon les besoins.

(1) D'autres compétences sont aussi définies par la FEMA ou dans la norme ISO 22361 : Vision stratégique et prise de décision; Leadership et influence; Communication de crise; Gestion d'équipe et collaboration; Résilience et bien-être; Adaptabilité et apprentissage continu; Intégrité, empathie et compassion; Autorité naturelle et capacité à inspirer confiance

Les rôles clés du leader en temps de crise

Un bon leader ne se contente pas de réagir, il agit avec clarté et détermination. Voici ses trois rôles majeurs :

- **Prendre des décisions rapides :** Dans le chaos, l'indécision est votre pire ennemi. Même une mauvaise décision vaut souvent mieux que l'absence de décision. Agissez vite, mais de manière éclairée.
- **Mobiliser les équipes :** En temps de crise, vous êtes le chef d'orchestre. Votre rôle n'est pas de jouer chaque instrument, mais de coordonner les efforts pour produire une symphonie harmonieuse malgré les désaccords.
- **Rassurer et inspirer :** Les crises sèment la peur et l'incertitude. Vos paroles et votre présence doivent apaiser, inspirer et redonner confiance. En montrant que vous êtes calme et résolu, vous donnez aux autres le courage de suivre votre exemple.

Dans une crise, un leader n'est pas seulement celui qui agit. C'est celui qui inspire, rallie et guide ses équipes avec une vision claire et une détermination inébranlable. Être à la hauteur de ce défi, c'est maîtriser l'art du leadership dans ses dimensions les plus exigeantes.

Différente phase impliquant un leader de crise

Dans la gestion de crise, le leadership joue un rôle crucial à travers différentes phases.

- **AVANT - Phase de prévention et préparation :** Cette phase initiale est cruciale pour établir les fondations d'une gestion de crise efficace.
- **PENDANT - Phase d'intervention :** La phase d'intervention représente le cœur de la gestion de crise, où la préparation est mise à l'épreuve face à une situation d'urgence réelle.
- **APRÈS - Phase de récupération et d'apprentissage :** La phase finale, bien que souvent négligée, est cruciale pour le développement à long terme de la résilience organisationnelle.

Ces trois phases constituent le cycle complet de la gestion de crise, chacune nécessitant des compétences de leadership spécifiques pour assurer une gestion efficace avant, pendant et après une crise.

AVANT : ANTICIPER L'IMPRÉVISIBLE

Le leadership de crise commence bien avant que l'imprévisible ne frappe.

Anticiper, c'est préparer son organisation à affronter les turbulences en identifiant les vulnérabilités et en développant une culture organisationnelle résiliente.

Cette approche proactive s'appuie sur trois piliers fondamentaux comprendre la nature des crises pour mieux en déceler les signaux avant-coureurs, bâtir une organisation agile et robuste capable de résister aux chocs, et adopter un leadership visionnaire pour inspirer et orienter les actions collectives.

En combinant ces leviers, les organisations peuvent non seulement réduire les incertitudes, mais également se positionner pour transformer les imprévus en opportunités de croissance et d'innovation.

Comprendre la nature des crises

Pour un leader de crise, anticiper les crises commence par une compréhension approfondie de ce qui les caractérise et par l'identification des signaux avant-coureurs. Si les crises surviennent souvent de manière imprévisible, elles sont souvent précédées de signaux faibles. Ces indices, tels qu'une baisse soudaine de la satisfaction client ou des tensions géopolitiques émergentes, offrent des fenêtres d'opportunité pour agir en amont.

L'exemple de Nokia. Malgré des signaux clairs sur l'obsolescence de son système Symbian, l'entreprise n'a pas su s'adapter à l'essor des smartphones avec l'arrivée de l'iPhone et d'Android. Persistant dans des stratégies dépassées, Nokia a continué à développer Symbian au lieu d'embrasser Android ou de concevoir un système d'exploitation compétitif, perdant ainsi son leadership sur le marché. À l'inverse, une veille stratégique proactive et l'identification des typologies de crises (financières, technologiques, réputationnelles) permettent de réduire les risques et d'éviter de tels scénarios.

Mener des analyses régulières des risques

Un leader adopte une approche méthodique pour identifier et évaluer les menaces potentielles. L'objectif est de réduire l'incertitude en mettant en place des mesures préventives.

- **Cartographier les risques :** Identifier les vulnérabilités internes (par exemple, des failles dans les systèmes informatiques ou des dépendances excessives à un seul fournisseur) et externes (changements réglementaires, tendances économiques ou environnementales).
- **Scénarios prédictifs :** Développer plusieurs scénarios possibles pour anticiper les impacts des crises potentielles. Par exemple, une entreprise de transport pourrait élaborer des stratégies pour réagir à une pénurie de carburant ou à une grève prolongée.
- **Surveiller les signaux faibles :** Mettre en place une veille stratégique pour détecter les premiers indices d'une crise à venir. Ces signaux faibles, comme des retards inhabituels dans la chaîne d'approvisionnement ou une hausse des plaintes clients, permettent de réagir avant que la situation ne dégénère.

Un exemple de Satya Nadella, PDG de Microsoft. Lorsqu'il a pris les rênes de l'entreprise en 2014, il a transformé Microsoft grâce à une stratégie proactive et visionnaire. Nadella a encouragé ses équipes à explorer de nouveaux marchés comme le cloud computing et l'intelligence artificielle tout en s'adaptant rapidement aux évolutions technologiques et à la concurrence accrue. Cette approche, fondée sur la veille et l'anticipation, a permis à Microsoft de prospérer dans un environnement compétitif et incertain, devenant une référence en matière de résilience organisationnelle.

Développer une culture organisationnelle résiliente

Une fois la nature des crises bien comprise, il devient crucial de bâtir une organisation capable de réagir efficacement à l'inattendu. Une culture organisationnelle solide constitue la pierre angulaire d'une gestion de crise efficace. Elle repose sur trois piliers essentiels :

- **Agilité :** Favoriser un environnement propice à l'innovation et à l'adaptabilité, où les équipes peuvent ajuster rapidement leurs actions face à des circonstances imprévues.
- **Communication proactive :** Mettre en place des protocoles clairs pour garantir des messages cohérents, précis et rassurants, tant en interne qu'en externe.
- **Formation continue :** Organiser régulièrement des simulations, des jeux de rôle et des analyses de crises passées pour préparer les équipes aux défis réels.

L'exemple de Toyota démontre l'importance de cette approche. Grâce à des protocoles détaillés et des processus rigoureux, l'entreprise a pu réagir rapidement lors de rappels de produits, préservant ainsi sa réputation malgré des crises d'envergure. Cette capacité à répondre efficacement aux situations critiques illustre l'importance d'une préparation méthodique et d'une culture organisationnelle orientée vers la résilience.

Former des équipes de crise composées de talents divers

Un leader avisé comprend que la gestion de crise est une tâche collective et nécessite des compétences variées. Former une équipe dédiée permet de maximiser la réactivité et l'efficacité en temps de crise.

- Diversité des talents : Une équipe de crise performante regroupe des experts issus de différents domaines (finances, communication, opérations, juridique, etc.), chacun apportant une perspective unique. Cette diversité favorise des solutions créatives et robustes face à des situations complexes.
- Rôles clairs et entraînements réguliers : Chaque membre doit connaître son rôle spécifique, et des simulations de crises doivent être organisées pour renforcer leur préparation. Par exemple, certaines entreprises mènent des exercices de « stress-test » pour évaluer leur réactivité face à des cyberattaques ou des interruptions majeures de la chaîne d'approvisionnement.

Renforcer la résilience

Un leader préventif ne se concentre pas uniquement sur les processus techniques, mais aussi sur le développement des compétences émotionnelles de ses équipes. La résilience organisationnelle repose largement sur la capacité des individus à gérer le stress, l'incertitude et les conflits.

- Développer l'empathie : Comprendre les besoins émotionnels des employés renforce la cohésion et la confiance au sein de l'organisation. Un environnement de travail où les gens se sentent soutenus est plus résistant face aux crises.
- Renforcer la gestion du stress : Proposer des formations sur la gestion de la pression et les mécanismes d'adaptation (par exemple, des ateliers sur la pleine conscience ou le coaching personnel) permet de préparer les équipes à des situations exigeantes. Un leader émotionnellement intelligent sert également de modèle en restant calme et lucide, même face à des défis.

Anticiper pour gérer, c'est investir dans la résilience organisationnelle et humaine. En formant des équipes solides, en développant des compétences émotionnelles et en anticipant méthodiquement les menaces, un leader visionnaire transforme l'incertitude en opportunité. C'est cette combinaison de préparation et d'agilité qui permet aux organisations de prospérer, même face à l'imprévisible.

PENDANT : AGIR AVEC CALME ET DÉTERMINATION

Pendant une crise, les leaders sont confrontés à une double exigence : agir rapidement et mobiliser efficacement leurs équipes dans un contexte d'incertitude extrême.

C'est une phase critique où les décisions et comportements du leader peuvent sceller le sort de l'organisation. Voici deux piliers fondamentaux du leadership pendant la crise.

La prise de décision sous pression

Lorsqu'une crise éclate, les leaders doivent prendre des décisions rapides, souvent avec des informations incomplètes ou contradictoires. Ces moments exigent sang-froid et discernement.

- **Établir des priorités :** Dans le chaos, il est essentiel de se concentrer sur les actions critiques. Une analyse rapide des enjeux prioritaires — sécurité des employés, continuité des opérations, protection des parties prenantes — aide à organiser une réponse structurée. Un leader efficace utilise des cadres décisionnels simples pour hiérarchiser les tâches et éviter la paralysie.
- **Éviter les biais cognitifs :** Sous pression, les biais tels que le biais de confirmation (privilégier des informations qui confirment ses hypothèses) ou l'aversion au risque peuvent nuire aux décisions. Impliquer des perspectives diverses, comme celles des experts ou des membres clés de l'équipe, réduit ces biais et améliore la qualité des choix.
- **Agir avec fermeté :** Dans une crise, l'inaction est plus risquée que la plupart des erreurs. Même une décision imparfaite peut donner une direction et rassurer les équipes. Une fois la décision prise, le leader doit la communiquer clairement et s'y engager.

Exemple : Jacinda Ardern, Première ministre de la Nouvelle-Zélande, a rapidement imposé des confinements stricts lors de la Covid 19, malgré le manque de données disponibles à ce moment-là. Bien que ces décisions aient été perçues comme radicales, elles ont permis à la Nouvelle-Zélande de limiter les infections et de préserver son économie à long terme. Son succès repose sur trois points clés :

- *La priorisation de la santé publique*
- *L'appui sur l'expertise scientifique*
- *Une communication claire et empathique*

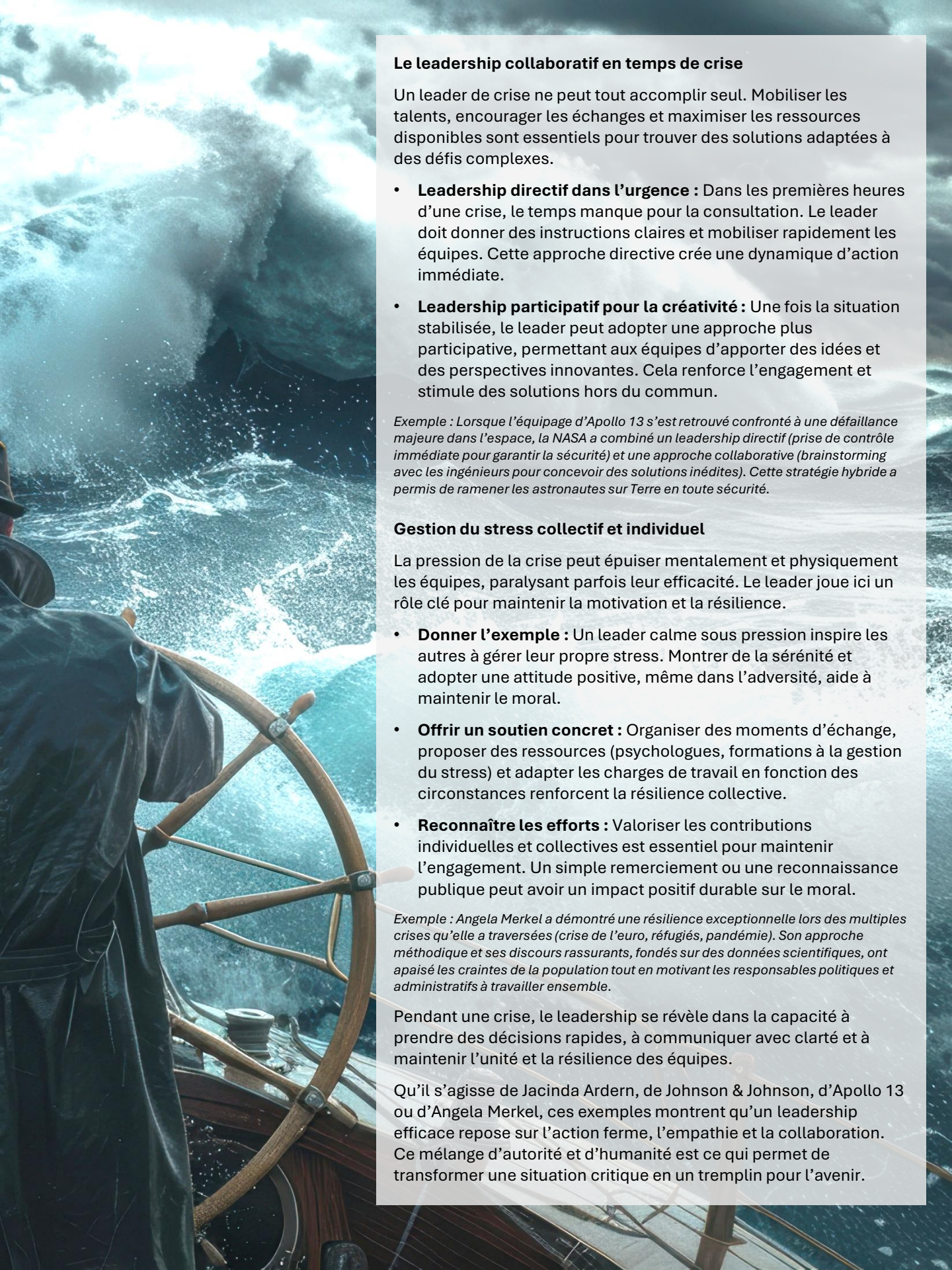
Son calme, sa clarté dans les messages et sa détermination ont renforcé la confiance du public, démontrant qu'un leadership décisif et humain peut transformer une crise en opportunité de protection et de résilience nationale.

Gérer la communication de crise

Pendant une crise, une communication efficace peut faire la différence entre le chaos et le contrôle. Un leader doit s'assurer que les bonnes informations atteignent les bonnes personnes au bon moment.

- **Clairvoyance :** En période d'incertitude, les faits doivent être communiqués de manière claire et compréhensible. Le leader doit éviter les ambiguïtés et répondre directement aux préoccupations des parties prenantes.
- **Empathie :** La crise affecte émotionnellement les employés, les clients et les partenaires. Reconnaître leurs craintes et montrer que l'organisation se soucie d'eux est crucial pour maintenir leur engagement.
- **Transparence :** Mentir ou minimiser l'impact d'une crise peut causer des dommages irréversibles à la réputation. Un leader transparent gagne la confiance, même en admettant des incertitudes ou des erreurs.

Exemple : En 1982, Johnson & Johnson a fait face à une crise majeure lorsque des capsules de Tylenol contaminées ont causé plusieurs décès. L'entreprise a rapidement rappelé ses produits, communiqué ouvertement sur les risques et renforcé les mesures de sécurité. Cette transparence proactive a sauvé des vies et préservé sa réputation.



Le leadership collaboratif en temps de crise

Un leader de crise ne peut tout accomplir seul. Mobiliser les talents, encourager les échanges et maximiser les ressources disponibles sont essentiels pour trouver des solutions adaptées à des défis complexes.

- **Leadership directif dans l'urgence :** Dans les premières heures d'une crise, le temps manque pour la consultation. Le leader doit donner des instructions claires et mobiliser rapidement les équipes. Cette approche directive crée une dynamique d'action immédiate.
- **Leadership participatif pour la créativité :** Une fois la situation stabilisée, le leader peut adopter une approche plus participative, permettant aux équipes d'apporter des idées et des perspectives innovantes. Cela renforce l'engagement et stimule des solutions hors du commun.

Exemple : Lorsque l'équipage d'Apollo 13 s'est retrouvé confronté à une défaillance majeure dans l'espace, la NASA a combiné un leadership directif (prise de contrôle immédiate pour garantir la sécurité) et une approche collaborative (brainstorming avec les ingénieurs pour concevoir des solutions inédites). Cette stratégie hybride a permis de ramener les astronautes sur Terre en toute sécurité.

Gestion du stress collectif et individuel

La pression de la crise peut épuiser mentalement et physiquement les équipes, paralysant parfois leur efficacité. Le leader joue ici un rôle clé pour maintenir la motivation et la résilience.

- **Donner l'exemple :** Un leader calme sous pression inspire les autres à gérer leur propre stress. Montrer de la sérénité et adopter une attitude positive, même dans l'adversité, aide à maintenir le moral.
- **Offrir un soutien concret :** Organiser des moments d'échange, proposer des ressources (psychologues, formations à la gestion du stress) et adapter les charges de travail en fonction des circonstances renforcent la résilience collective.
- **Reconnaître les efforts :** Valoriser les contributions individuelles et collectives est essentiel pour maintenir l'engagement. Un simple remerciement ou une reconnaissance publique peut avoir un impact positif durable sur le moral.

Exemple : Angela Merkel a démontré une résilience exceptionnelle lors des multiples crises qu'elle a traversées (crise de l'euro, réfugiés, pandémie). Son approche méthodique et ses discours rassurants, fondés sur des données scientifiques, ont apaisé les craintes de la population tout en motivant les responsables politiques et administratifs à travailler ensemble.

Pendant une crise, le leadership se révèle dans la capacité à prendre des décisions rapides, à communiquer avec clarté et à maintenir l'unité et la résilience des équipes.

Qu'il s'agisse de Jacinda Ardern, de Johnson & Johnson, d'Apollo 13 ou d'Angela Merkel, ces exemples montrent qu'un leadership efficace repose sur l'action ferme, l'empathie et la collaboration. Ce mélange d'autorité et d'humanité est ce qui permet de transformer une situation critique en un tremplin pour l'avenir.

APRÈS : RECONSTRUIRE ET CAPITALISER SUR LES LEÇONS

Lorsque la tempête est passée, le travail du leader ne s'arrête pas à célébrer la survie de l'organisation. La phase post-crise est un moment clé pour reconstruire, tirer des enseignements et préparer l'avenir.

C'est dans cette période que les leaders de crise se distinguent par leur capacité à transformer les défis en opportunités et à insuffler une nouvelle dynamique. Gérer cette phase avec efficacité nécessite une approche réfléchie, structurée et inspirante.

Gérer la phase post-crise

Après une crise, la priorité est d'évaluer l'impact des événements et de poser des bases solides pour la reconstruction. Cette phase doit être marquée par une grande honnêteté et une communication transparente.

- **Faites un bilan honnête des pertes et des gains :** Évaluer objectivement les pertes, qu'elles soient financières, humaines ou stratégiques, est essentiel pour comprendre les conséquences réelles de la crise. En parallèle, identifiez les réussites, même modestes, pour souligner les forces qui ont permis à l'organisation de surmonter l'épreuve.
- **Restaurez la confiance avec transparence :** Admettre les erreurs, expliquer les actions mises en œuvre pour y remédier et partager les leçons tirées de la crise sont des éléments fondamentaux pour regagner la confiance des parties prenantes. Une communication honnête et claire montre que l'organisation a non seulement survécu, mais qu'elle en ressort plus forte.

Exemple : Après la catastrophe environnementale de 2010, BP a adopté une démarche proactive en investissant massivement dans des projets communautaires et environnementaux (1 milliard USD pour la restauration des ressources naturelles). En parallèle, l'entreprise a renforcé ses protocoles de sécurité et collaboré avec les parties prenantes pour montrer son engagement à ne pas répéter les mêmes erreurs. Cette transparence et ces actions concrètes ont contribué, au fil des années, à regagner une partie de la confiance perdue.

Évaluer l'impact de la crise

Un bilan détaillé est essentiel pour comprendre ce qui a fonctionné et ce qui a échoué pendant la crise. Cette analyse est le point de départ pour éviter les erreurs du passé et préparer un avenir plus résilient.

- **Analyse rétrospective :** Il est indispensable de revisiter chaque étape de la gestion de crise pour analyser les décisions prises, les résultats obtenus et les lacunes identifiées. Cette rétrospective doit être menée de manière objective, en impliquant toutes les parties concernées, afin de garantir un retour d'expérience complet et riche.
- **Impacts mesurables :** Quantifiez les pertes financières, évaluez les dommages sur la réputation et mesurez la satisfaction des employés, des clients et des partenaires. Ces données permettent de prioriser les domaines nécessitant des améliorations ou des investissements.
- **Capitaliser sur les enseignements :** L'apprentissage est la clé de la résilience. Utilisez les leçons tirées de la crise pour renforcer vos processus, introduire de nouvelles pratiques et ajuster votre gouvernance.

L'exemple des grandes institutions bancaires après la crise de 2008 montre que même les événements les plus dévastateurs peuvent être des catalyseurs de progrès. Ces banques ont introduit des mécanismes de régulation et des stratégies de gestion des risques plus robustes, renforçant ainsi leur stabilité.

Transformer les crises en opportunité

Une crise, bien qu'éprouvante, peut devenir une opportunité de transformation. C'est souvent dans ces moments que les organisations repensent leurs modèles, adoptent des pratiques plus résilientes et se réinventent pour mieux prospérer.

- **Implémenter de nouvelles pratiques :** Les leçons apprises doivent être intégrées dans les processus organisationnels. Cela peut inclure des changements dans les protocoles de gestion des risques, l'amélioration des systèmes de communication ou la mise en place de formations pour préparer les équipes à de futures crises.
- **Revoir les structures organisationnelles :** Une crise révèle souvent des failles dans la structure et la gouvernance d'une organisation. Le leader doit évaluer si des ajustements, tels que des chaînes de commandement plus claires ou des systèmes plus agiles, sont nécessaires pour améliorer la réactivité.
- **Créer une vision inspirante :** Après une crise, les employés et les partenaires ont besoin d'un cap clair pour avancer. Le leader doit transformer les échecs en tremplins, montrant que les défis surmontés renforcent l'organisation. Inspirer une vision ambitieuse et positive aide à mobiliser les énergies pour le futur.

Exemple : Lorsque les ventes de DVD ont commencé à décliner, Netflix a saisi l'opportunité de pivoter vers le streaming en ligne. Ce virage stratégique, rendu possible par une vision innovante et un leadership audacieux, a permis à l'entreprise non seulement de survivre à la transition numérique, mais aussi de devenir un acteur dominant de l'industrie du divertissement.

Le rôle du leader après la crise

Une fois la crise passée, le style de leadership doit évoluer pour répondre aux nouveaux besoins de l'organisation. Le leader doit trouver un équilibre entre stabilisation et projection vers l'avenir.

- **Reprendre un leadership classique :** Pendant une crise, le leadership est souvent directif et centré sur l'urgence. Après la crise, le leader doit redonner de l'autonomie aux équipes et favoriser un retour à une gouvernance participative. Cela aide à stabiliser l'organisation et à restaurer un climat de normalité.
- **Capitaliser sur les leçons apprises :** Transformez les expériences de crise en avantages stratégiques. Identifiez les nouvelles compétences acquises, les opportunités créées et les forces révélées pendant la crise, et intégrez-les dans la stratégie organisationnelle.
- **Inspirer une vision d'avenir :** Une crise n'est pas seulement un événement à surmonter, c'est un moment pour redéfinir la direction de l'organisation. Le leader doit articuler une vision inspirante qui donne un sens aux efforts fournis et mobilise les équipes pour aller de l'avant avec confiance et ambition.

La période post-crise est un moment décisif pour les organisations. Elle exige du leader non seulement une capacité à stabiliser et reconstruire, mais aussi une vision stratégique pour transformer les défis en opportunités. En gérant la phase post-crise avec transparence, en capitalisant sur les leçons apprises et en innovant pour l'avenir, un leader peut non seulement restaurer la confiance, mais aussi poser les bases d'une organisation plus résiliente et prospère.

Les crises ne définissent pas les organisations : ce sont les réponses qu'elles y apportent et les transformations qu'elles opèrent qui les distinguent. Le véritable leadership se mesure non pas dans la survie, mais dans la capacité à rebondir plus fort et à inspirer un avenir meilleur.

EN CONCLUSION DE CE DOSSIER

Dans un monde marqué par l'incertitude et les transformations rapides, le leadership de crise se révèle être une compétence incontournable.

Les crises, bien qu'éprouvantes, offrent aussi une opportunité unique de démontrer une résilience exemplaire, de mobiliser des équipes avec conviction et de transformer les défis en leviers d'innovation.

Un leadership de crise efficace repose sur trois piliers fondamentaux :

- **Anticiper pour protéger :** La préparation en amont, qu'il s'agisse de comprendre la nature des crises, d'identifier les vulnérabilités ou de développer une culture organisationnelle résiliente, est essentielle pour amortir les chocs et assurer la continuité.
- **Agir avec clarté sous pression :** Les moments critiques exigent des décisions rapides et stratégiques, une communication empathique et transparente, ainsi qu'une capacité à maintenir l'unité et la motivation des équipes face à l'adversité.
- **Rebondir et transformer :** Une fois la crise surmontée, le rôle du leader est de tirer les leçons de l'expérience, de reconstruire avec transparence et de projeter une vision inspirante pour l'avenir, transformant ainsi chaque défi en une opportunité de croissance.

Les grands leaders ne se contentent pas de survivre : ils saisissent la crise comme une opportunité pour ce ré-inventer

Comme l'ont montré des exemples inspirants tels que Satya Nadella chez Microsoft ou Jacinda Ardern en Nouvelle-Zélande, c'est par des actions déterminées et un esprit de transformation que les organisations se relèvent plus fortes.

En fin de compte, le leadership en temps de crise n'est pas seulement une affaire de compétences, c'est un état d'esprit. Celui de rester ferme dans la tempête, d'inspirer quand tout vacille, et d'oser bâtir un futur meilleur.

Karine Maréchal-Richard

Consultante et formatrice experte en continuité des affaires et gestion de crise j'accompagne les organisations pour développer leur résilience face aux perturbations majeures.

www.crise-resilience.com

CRISE & RÉSILIENCE
L'ART DE SURVIVRE AUX CRISES

"Le leadership ne subit pas la crise : il la réécrit ..."

Karine Maréchal-Richard

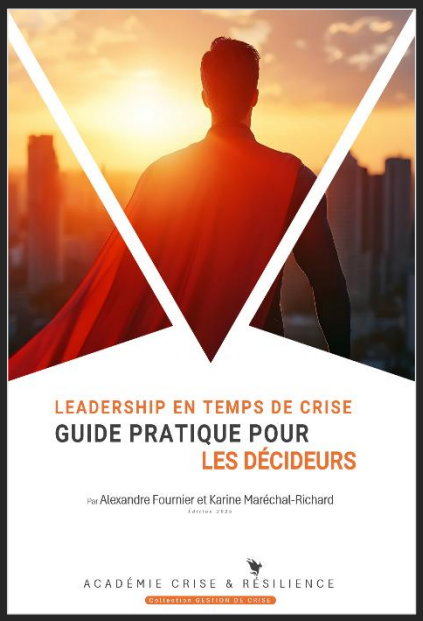
Quel type de leader de crise êtes-vous ?

Testez-vous pour identifier vos forces et les domaines à développer afin d'optimiser votre efficacité en tant que leader face aux défis complexes.

Télécharger le test

www.academiecriseetresilience.com/outils

Sortie prochaine du livre



Envie de recevoir ce livre...

Pré-inscription

www.academiecriseetresilience.com/livres

CRISE & RÉSILIENCE C'EST... AUSSI

Une chaîne YouTube avec...

Des conférences et formations gratuites

Des interviews d'experts :

Des réponses à vos questions :

https://www.youtube.com/criseetresilience

Une page LinkedIn avec...

Des billets d'actualités, des guides, des astuces, de l'humour, des articles...

https://www.linkedin.com/company/crise-et-r%C3%A9silience/

Des formations ACADEMIE CRISE & RÉSILIENCE sur...

La gestion de crise, la simulation de crise, la continuité des affaires, la reprise informatique, l'intelligence artificielle, etc.

https://www.academiecriseetresilience.com/

En complément à ce magazine

Voici des Magazines et podcasts intéressants

Découvrez Cyber-IT Mag, votre compagnon idéal pour naviguer dans l'univers de la Cyber et l'IT.

Que vous soyez un professionnel ou simplement curieux, les sujets sont accessibles à tous ! La cyber est un marathon pas un sprint !

https://www.linkedin.com/company/cyber-it-magazine/posts/?feedView=all

Née il y a 10 ans, la revue Sécurité & Défense magazine répond au besoin éditorial reflétant le continuum sécurité & défense. Revue bimestrielle haut de gamme, elle joue la carte de l'influence au travers d'une ligne éditoriale marquée.

https://www.linkedin.com/company/s-d-magazine/posts/?feedView=all

Face au Risque, le média de référence des responsables de la sécurité. En vous donnant les clés de transformations et mutations de votre secteur, en vous guidant grâce aux sélections des meilleurs pratiques, Face au risque est le média d'actualités et le seul centre de ressources avec comme objectif et ambition : Faire entendre la parole d'experts sur les grands enjeux de la sécurité.
https://www.linkedin.com/company/face-au-risque/

Le magazine *True North Resilience* est une publication de Disaster Recovery Institute Canada destinée à ses professionnels certifiés.

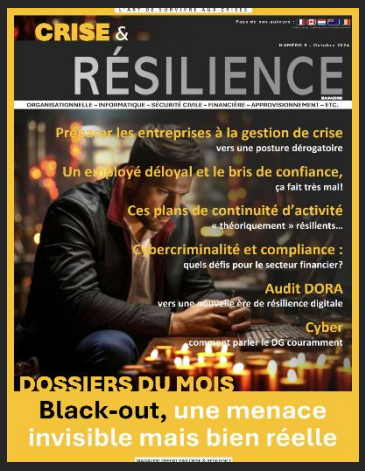
Ce magazine est publié deux fois par an, avec trois numéros publiés à ce jour. Les professionnels certifiés peuvent accéder aux magazines et articles ici, via le *Knowledge Garden* ou la bibliothèque du DRII.

Podcast francophone sur la cybersécurité. Pour professionnels et curieux.

https://www.linkedin.com/showcase/polysecure/posts/?feedView=all

Envie de partager votre magazine.
Contactez-moi à info@crise-resilience.com

Numéros déjà parus



ABONNEZ-VOUS ICI

Ou ici 👉 www.magazinecriseetresilience.com

Prochaines formations

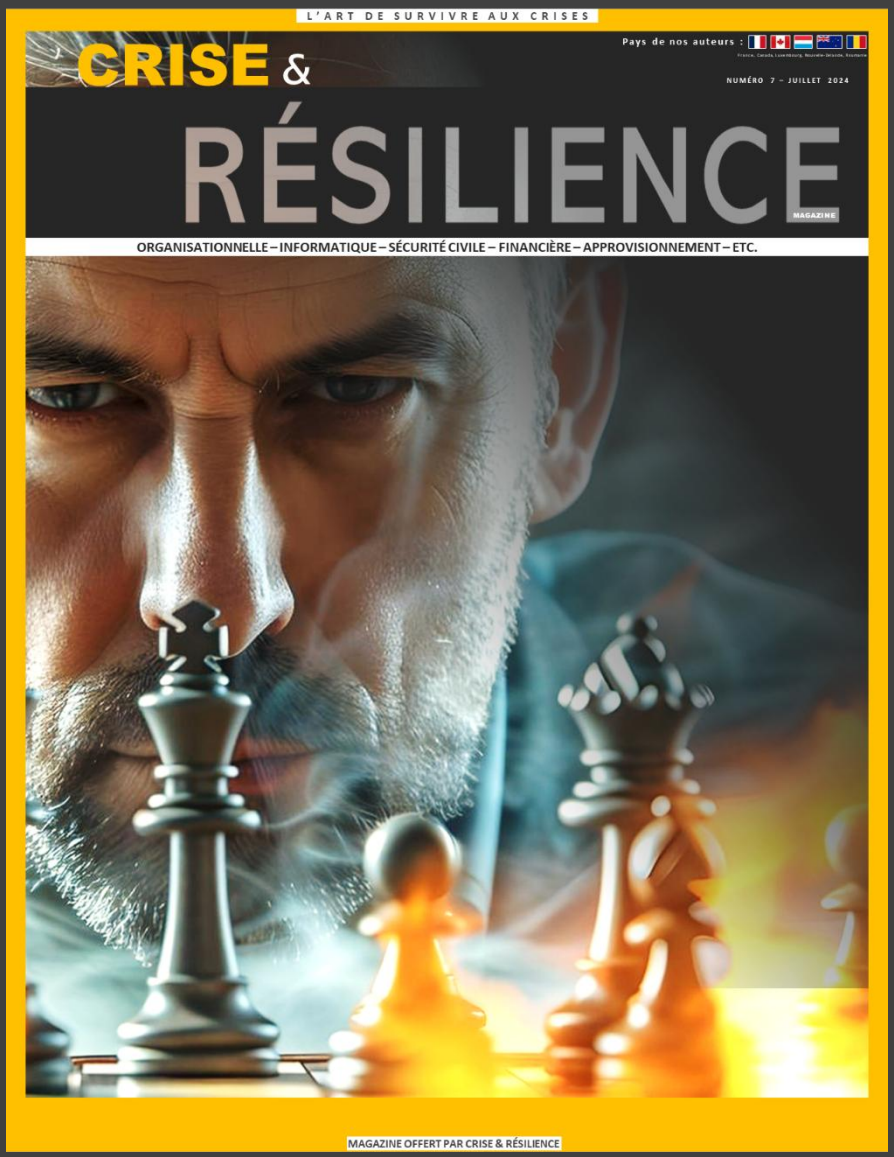
Académie **Crise & Résilience**

Oui vous avez bien lu...

Nos formations ont une garantie!

www.academiecriseetresilience.com

RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

www.CriseEtResilience-Magazine.com