

RÉSILIENCE

MAGAZINE

ORGANISATIONNELLE – INFORMATIQUE – SÉCURITÉ CIVILE – FINANCIÈRE – CHAÎNE D'APPROVISIONNEMENT – ETC.

Intelligence artificielle

Interview d'une experte en intelligence artificiel sur l'utilisation de l'IA en gestion de crise

Biais cognitifs

Dans la mise en place de la cybersécurité et dans les cellules de gestion de crise

Négociation

Pourquoi il est possible de négocier lors d'une cyberattaque

Opportunité

Le management des opportunités face aux nouvelles crises

OUTIL leadership

Quelle leader êtes vous en période de crise

Dernière minute!

Quand les pirates mécontents jettent l'ancre face à la réforme des retraites.

PARRAIN DE CE NUMÉRO

RAPHAËL DE VITTORIS

INTERVIEW :
RÉSILIENCE ET ANTIFRAGILITÉ,
POUR UNE ENTREPRISE PROSPÈRE



DOSSIER DU MOIS

Fragilité des chaînes d'approvisionnement

SOYEZ RÉSILIENT

JANVIER – AVRIL – JUILLET – OCTOBRE

Rejoignez-nous
sur LinkedIn 

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

Pour aider les organisations et les entreprises à se préparer à la crise et à trouver des moyens de s'adapter et de se développer, nous sommes fiers de vous offrir ce magazine consacré à la gestion de crise, à la résilience organisationnelle et à la survie des entreprises en période de crise.

Ce magazine trimestriel vous offre des articles, des outils, des interviews et des dossiers sur le sujet. Nous vous donnons aussi les astuces et les stratégies nécessaires pour vous préparer à survivre à événement majeur et y survivre.

Abonnez-vous dès aujourd'hui pour profiter de tous nos conseils et outils en matière de gestion de crise et de résilience organisationnelle. Faites le choix de la sécurité et de la pérennité pour votre entreprise!

Et en plus, c'est gratuit!



Pour vous abonner cliquez ici 
ou allez sur www.crise-resilience.com/magazine



Raphaël de Vittoris
 Founder Antifragile.fr
 Michelin Group Crisis
 Manager - Associate
 Professor Strategy & Crisis
 Mgt Université Clermont
 Auvergne

Pour ce nouveau numéro, j'ai l'honneur de vous partager mon interview portant sur l'antifragilité, où la menace se transforme en opportunité. Ce thème est en rapport avec l'article de Karine Maréchal-Richard, qui démontre l'importance de tirer un bénéfice d'une mise à l'épreuve au moyen des exercices de crise, mais aussi avec celui de Christophe Saussereau où, au-delà de la seule résilience à l'évènement, des opportunités peuvent émerger de la crise.

L'antifragilité peut se définir comme la recherche de l'optionnalité et la quête de redondance, qui fait totalement sens lorsqu'on évoque les chaînes d'approvisionnement et l'impact de leur arrêt, comme cela est démontré dans le dossier du mois. Toutefois, si ces notions sont aisément assimilables pour les entreprises préparant leurs dispositifs de gestion de crise, qu'en est-il des communes et de leur préparation? Guillaume Aghroum nous offrira une grille de lecture à ce propos.

La technologie apporte de nouvelles perspectives à la gestion de crise et aux potentialités de résilience ou d'antifragilité. C'est dans ce cadre que la notion de « digitalisation » ou « transformation numérique » sera abordée via un article d'Alexandre Fournier sur l'impact de l'intelligence artificielle sur la discipline et un article de Lilian Laugerat sur la négociation en situation de cyberattaque. Cette digitalisation contribue au transfert des informations, point clé de la gestion de crise, comme l'explique Hervé Jouffre dans son article.

Vous l'avez compris, le thème de ce numéro est de commencer à songer à tirer parti de la volatilité plutôt que de seulement se préparer à résister à l'aléa.

Comprendre la résilience et l'antifragilité pour passer de l'un à l'autre selon le contexte.

Devenir plus pérenne.

Survivre...

sommaire

Numéro 2 – AVRIL 2023

- PARÔLE D'EXPERT : Résilience et antifragilité** **04**
 Raphaël de Vittoris
Interview fait par Alexandre Fournier, article écrit par Karine Maréchal-Richard
- L'expression des biais cognitifs dans les cellules de crise** **08**
par Raphaël de Vittoris
- Pourquoi est-il possible de négocier lors d'une cyberattaque** **12**
par Lilian Laugerat
- Le management des opportunités face aux nouvelles crises** **16**
par Christophe Saussereau
- La crise ne frappe pas avant d'entrée!** **20**
 6 raisons d'effectuer des exercices de gestion de crise
par Karine Maréchal-Richard
- SECRET : 16 secrets d'un exercice de gestion de crise réussi** **24**
par Karine Maréchal-Richard
- LE DOSSIER DU MOIS : La chaîne d'approvisionnement** **26**
par Alexandre Fournier
- CONFÉRENCE : Comment bien rater sa gestion de crise** **37**
par Alexandre Fournier
- Gestion de crise : qui prépare les communes ?** **38**
par Guillaume Aghroum
- OUTIL GRATUIT : Auto-évaluation de votre résilience** **41**
- Le nerf de la guerre c'est le renseignement** **42**
par Hervé Jouffre
- SENSIBILISATION : 15 affiches offertes** **45**
- INTERVIEW : La gestion de crise à l'ère de l'I.A.** **46**
 Avantages, limites et risques
par Alexandre Fournier
- Les biais cognitifs qui nous empêchent d'agir** **52**
par Romain Bouvet
- CHRONIQUE CYBERSÉCURITÉ : Démystifier les tests d'intrusion** **56**
par CyberSwat
- LA GAZETTE : Les pirates seniors en grève** **58**
par Anne Honym



Chers lecteurs et lectrices,

C'est avec un immense plaisir et une grande fierté que nous vous présentons notre deuxième numéro! Quelle aventure extraordinaire que celle de concocter ce magazine pour vous, chaque trimestre. Nous sommes ravis de collaborer étroitement avec nos talentueux auteurs, qui partagent leurs passions et leur générosité sans compter à travers leurs articles captivants. Nous tenons à adresser un immense merci à toutes les personnes qui ont pris le temps de nous envoyer leurs précieux commentaires sur notre premier numéro. Vos retours d'expérience nous sont très chers, car ils nous permettent d'améliorer sans cesse notre magazine et de vous offrir un contenu toujours plus pertinent et inspirant. Vous êtes tout simplement GÉNIAUX!

Nous attendons avec impatience de lire vos impressions sur ce nouveau numéro. N'hésitez pas à nous faire part de vos coups de cœur, de vos réflexions et de vos suggestions. Ensemble, continuons à faire grandir cette belle aventure. Profitez de chaque page et savourez ces moments de partage!

Nous vous souhaitons une lecture chaleureuse et enrichissante.

Alexandre et Karine

Résilience et antifragilité, pour une entreprise prospère



Interview

Raphaël de Vittoris

Founder Antifragile.fr

Michelin Group Crisis Manager -
Associate Professor Strategy &
Crisis Mgt Université Clermont
Auvergne



La splendeur et la finesse d'un plat en porcelaine sont remarquables, mais il est surtout très fragile. Lorsqu'il tombe, il se brise facilement.

En revanche, un plat en plastique, même s'il est moins esthétique que la porcelaine, est résistant aux chocs. Il pourra y avoir quelques bosses, mais, on pourra continuer à l'utiliser.

La fragilité et la robustesse sont deux termes opposés.

Mais comment appelle-t-on quelque chose qui ressort plus grand, plus vigoureux, plus fort après un choc ?

De l'antifragilité.

Interview par Alexandre Fournier



Expert en gestion et simulation de crise

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

Article écrit par Karine Maréchal-Richard



Experte en continuité des affaires et gestion de crise

Consultante, formatrice et conférencière dans les domaines de la continuité des affaires et de la gestion de crise depuis 15 ans.



Lorsqu'un enfant apprend à marcher, il fait une première chute, puis une seconde. Il a quelques bosses, mais cela ne l'empêche pas de se relever et de faire des apprentissages. Il va développer des techniques et des réflexes qui vont lui permettre d'être plus habile, d'être plus sûr dans ses déplacements et, surtout, il saura comment éviter les prochaines chutes. Raphaël De Vittoris explique l'antifragilité comme étant un monde que l'on explore un peu comme un petit enfant qui découvre et apprend à marcher.

“ L'échec est un diplôme ”

Raphaël De Vittoris

Effectivement, les échecs et les erreurs sont des apprentissages. Ils nous conduisent à trouver des solutions pour faire face à des chocs, à du stress, à des erreurs, à de l'incertitude ou à tout autre événement perturbateur. L'incertitude nous permet de développer des savoirs. C'est ça, l'antifragilité.

Avec la mondialisation croissante des échanges et la dépendance à l'égard de la technologie, les entreprises doivent faire face à des risques toujours plus nombreux et variés. Les changements climatiques ont également ajouté une dimension supplémentaire aux risques auxquels les entreprises sont confrontées, avec des événements météorologiques extrêmes de plus en plus fréquents et imprévisibles. De plus, les épidémies ou les pandémies mondiales comme celle de la COVID-19 ont montré à quel point les entreprises peuvent être vulnérables à des événements qui échappent à leur contrôle.

Les perturbations économiques, les restrictions de voyage et les mesures de confinement ont perturbé les activités des entreprises et entraîné des pertes financières importantes. Des événements géopolitiques tels que la guerre entre l'Ukraine et la Russie peuvent également avoir un impact significatif sur les entreprises.

Les entreprises qui dépendent fortement de l'exportation ou de l'importation de biens et de services peuvent être particulièrement vulnérables à ces événements.

Tous ces facteurs contribuent à rendre les entreprises plus fragiles et à leur donner l'impression qu'une épée de Damoclès est suspendue au-dessus de leur tête.

Un simple grain de sable, comme une panne de courant ou une cyberattaque, peut perturber considérablement le fonctionnement normal d'une entreprise et lui causer des pertes financières importantes. Il est donc crucial pour les entreprises de prendre en compte ces risques et de mettre en place des mesures pour atténuer leur impact potentiel.



C'est là qu'entre en jeu le concept de résilience. La résilience, c'est absorber un choc, y résister, le surmonter, ou l'affronter pour revenir dans un état de quasi-normalité.

Pour y parvenir, les entreprises doivent élaborer des plans de continuité des affaires, de gestion de crise, de reprise informatique, etc., et traverser la turbulence avec détermination. En mettant en place de la résilience dans les entreprises, elles limitent de nombreux points de fragilité.

Bien que la résilience et l'antifragilité partagent certains points communs comme faire face à des chocs ou des à perturbations, il y a quelques contraintes à prendre en compte pour élaborer des stratégies organisationnelles en cas de choc.

A graphic for an interview. It features a large portrait of Raphaël De Vittoris on the left, wearing glasses and a dark shirt, against a background of glowing blue and green network lines. On the right, there is a smaller inset photo of him in a white shirt. Below the main portrait, the text reads 'INTERVIEW PAROLE D'EXPERTS' and 'ANTIFRAGILITÉ : Comment Transformer les Menaces en Opportunités ?'. At the bottom right, his name 'Raphaël De Vittoris' is written, followed by his credentials: 'Michelin Group Crisis Manager - Lecturer in Crisis Management & Strategy PhD in Management Science - Université Le Havre Normandie'. A yellow arrow points from the text in the previous block towards this graphic.

Écoutez l'interview complet de Raphaël de Vittoris

La première contrainte concerne les notions de risque et d'incertitude. En effet, le concept de résilience est compatible uniquement avec la notion de risque. Afin de rendre une entreprise résiliente, il est nécessaire de réaliser une analyse des risques qui permet d'évaluer la probabilité et l'impact des risques, afin de prendre les mesures nécessaires pour réduire leur apparition et leurs conséquences. En revanche, le concept de résilience est inadapté pour traiter l'incertitude. Tout comme son nom l'indique, l'incertitude ne peut être mesurée par des probabilités, contrairement aux risques qui sont mesurables.

La deuxième contrainte est la suivante : si le concept de résilience s'est résister à un choc, il ne faut pas que cela empêche l'entreprise de développer une adaptabilité aux évolutions.

Est-ce que l'entreprise doit être uniquement résiliente ou antifragile ou bien une combinaison des deux ?

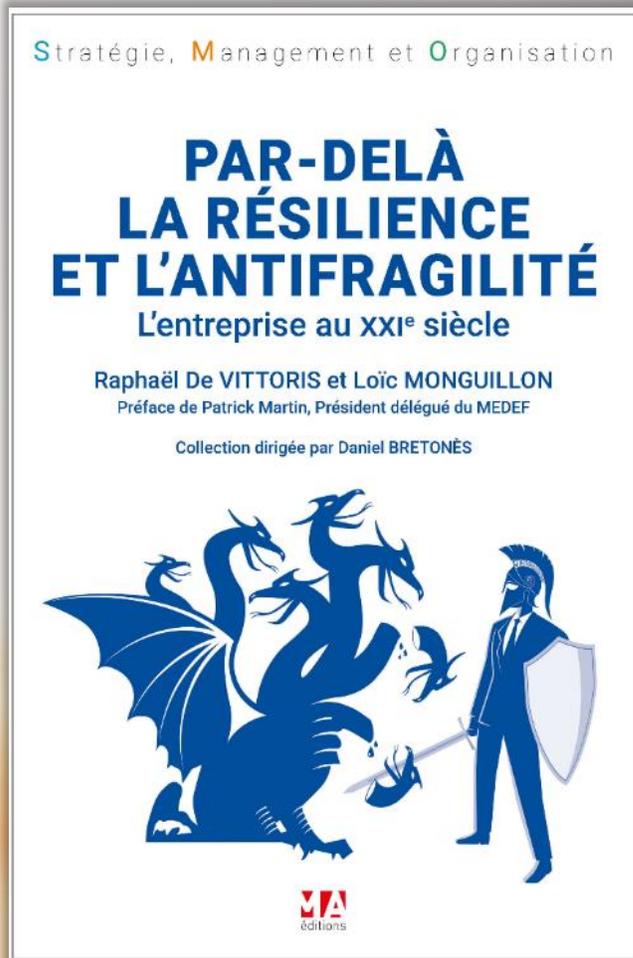
Pour être pérennes, les entreprises doivent développer à la fois la résilience et l'antifragilité. Selon leur domaine d'activité et la situation, les entreprises devront mettre en place des stratégies pour renforcer leur résilience à certains moments et, à d'autres, elles devront adopter des stratégies axées sur l'antifragilité. En fait, il s'agit d'un « patchwork » des deux concepts qui doivent être appliqués à tous les niveaux de l'entreprise.

Il est crucial de trouver un équilibre entre ces deux approches si l'entreprise souhaite être pérenne. Raphaël De Vittoris parle d'une mosaïque pérenne.

Trouver l'équilibre parfait entre résilience et antifragilité est la clé de la pérennité.

En conclusion, la fragilité et la robustesse ne suffisent plus. L'avenir appartient à l'antifragilité. Les entreprises doivent être conscientes des risques croissants liés à la mondialisation et aux changements climatiques, et accueillir l'incertitude comme une opportunité de se développer. Pour réussir, elles doivent être à la fois être résilientes et antifragiles. La résilience aide à surmonter un choc, mais c'est l'antifragilité qui permet de prospérer après. Les entreprises doivent élaborer des plans de continuité des affaires, mais également apprendre des échecs et des erreurs pour être plus habiles et plus à même de faire face aux perturbations.

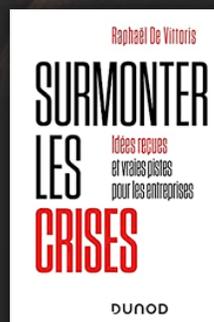
En savoir plus sur l'antifragilité



Dans ce livre, vous découvrirez les éléments essentiels pour ajuster votre entreprise à un environnement fluctuant, imprévisible, compliqué et équivoque.

Une approche novatrice vous sera proposée pour repenser votre structure organisationnelle et renforcer ses qualités fondamentales, permettant ainsi d'assurer sa pérennité et sa croissance sur le long terme.

Autre livre du même auteur :



Livres à lire



Vidéos à voir



L'expression des biais cognitifs dans les cellules de crise



Depuis les productions de Kahneman et Tversky (1972), il n'est pas rare de voir aborder la problématique des facteurs humains et notamment de l'expression des biais cognitifs dans le cadre des études de crises.

Pourtant, ils sont rarement listés et explicités.

par Raphaël de Vittoris



Founder Antifragile.fr
Michelin Group Crisis Manager –
Associate Professor Strategy & Crisis Mgt
Université Clermont Auvergne



La gestion d'une crise nécessite de pouvoir se reposer sur une organisation, sur des méthodes et des outils, mais aussi sur une capacité aigüe à des interprétations et des décisions, comme l'a démontré Weick entre 1988 et 2010. Dans ce cadre, connaître et comprendre les biais qui s'expriment en nous en situation de crise devient un levier clé du succès de la gestion de l'événement.

Pour pallier le manque de précision quant aux biais observés en cellule de crise, nous vous proposons un panel des biais fréquemment identifiés en cellule et quelques astuces pour les éviter.

L'observation de diverses cellules de crise en action nous a en effet amenés à identifier trois vecteurs nourrissant l'expression de ces biais :

L'expérience :

aussi profonde et riche est-elle, toute expérience est par définition limitée.

Cette limitation, associée à son pouvoir de représentation personnelle, amène à un effet ciseau (couple limitation-influence) particulièrement favorable à l'expression des biais cognitifs.

Le statut hiérarchique :

la légitimité est très souvent associée au statut hiérarchique de la personne dans de nombreuses organisations aussi bien privées que publiques.

Il apparaît très difficile tant aux détenteurs des titres qu'aux interlocuteurs de ces responsables de dissocier le statut (grade, position, etc.) des notions de pertinence des propositions au statut.

La planification :

la planification, lorsqu'elle tend vers le détail selon une description précise et anticipée des crises à venir et qu'elle se base sur le respect de routines solides, semble contribuer à la réduction de l'ouverture cognitive, à l'anticipation de ruptures potentielles et à l'amorce d'actions improvisées.

**« Les biais cognitifs
brouillent nos décisions.
Nous nous reposons trop
lourdement sur les jugements
machinaux, intuitifs, et même
lorsque nous nous efforçons
d'établir un raisonnement,
notre logique est souvent
paresseuse ou erronée. »**

Soll et al.



Nous proposons ici de nous intéresser aux neuf biais cognitifs que nous observons le plus souvent en situation de crise et qui faussent la compréhension et la prise de décision des cellules de crise :

Le biais de narration :

phénomène de sélection d'éléments jugés a posteriori afin qu'ils s'articulent dans un récit qui nous apparaît cohérent. La raison du sujet manifestant ce biais est moins intéressée par la vérité des faits, avec ses parts de clarté et d'inconnu, que par une logique apparente laissant apparaître une continuité logique, car causale, dût-elle être fautive. C'est dans ce cadre que tout narratif décrivant une crise une fois l'événement passé peut être un gage de cohérence, mais aucunement de vérité.

Le biais du survivant :

toute expérience d'autres crises amène un risque de généraliser les situations de crise précédentes considérées comme satisfaisantes, voire réussies. Or les situations étant toutes différentes, cela peut amener à répéter aveuglément des routines et des principes potentiellement inadaptés, voire contre-productifs. Ici, l'induction peut donc amener à stéréotyper les réponses et les décisions au regard de situations apparemment comparables, mais réellement très distinctes.

Le biais du champion :

il s'exprime comme un excès de confiance envers des positions légitimes et expertes sans prendre en considération que les « champions », s'ils disposent de connaissances spécifiques évidentes, sont enclins à des biais idiosyncrasiques réduisant l'anticipation et l'imagination.

Le biais de représentativité :

les événements qui nous viennent plus facilement en mémoire, du fait de leur fréquence ou bien de leur caractère marquant, nous semblent plus plausibles, voire probables, que d'autres. Le phénomène d'induction est ici encore à l'œuvre et conduit à surestimer les potentialités de risques dans une subjectivité tout inductive.

ENTRAÎNEZ-VOUS POUR ÉVITER LES PHRASES.

Si l'expression des biais n'est pas contrôlable, il demeure qu'une connaissance des biais par l'équipe de la cellule de crise permet de détecter leur manifestation de manière à en diminuer l'influence.

À ce titre, nous conseillons aux cellules de s'interdire de prononcer ou d'entendre de telles phrases en situation de crise :

« **Voici comment tout cela est arrivé, c'est tout simple :...** »

« **C'est une situation bien connue :...** »

« **Restons sur des méthodologies utilisées par ceux qui ont fait face avec succès à de telles circonstances.** »

« **Suivons le plan à la lettre, c'est bien assez.** »

« **Je connais bien la gestion de crise, j'ai fait toute ma carrière dans l'armée/la police/les forces d'intervention/etc.** »

« **Je savais que la décision était stupide... Mais, comme tout le monde était d'accord, je n'ai pas voulu dire quoi que ce soit.** »

« **Je vous propose d'abord mon idée et vous réagissez ensuite.** »

« **Ils n'auraient jamais dû faire ça à ce moment.** »

« **J'ai rapidement collecté quelques informations et voici la situation :...** »

Le biais de présomption :

il s'agit d'un phénomène consistant à présumer que l'on comprend une problématique du seul fait que l'on dispose d'une routine pour la gérer. Ce biais conduit le plus souvent à un excès de confiance dans le protocole et limite, par conséquent, la conservation d'une marge de manœuvre et d'adaptabilité.

Le biais d'attribution :

ce phénomène consiste à attribuer les succès des décisions et des actions à ses qualités personnelles et à attribuer ses échecs au hasard. Ce biais s'exprime de façon particulièrement significative lors des séances de retour d'expérience.

Le biais d'ancrage :

il consiste à instaurer les termes du débat et ainsi à influencer la réponse de l'interlocuteur. Il est particulièrement observable lors de discussions et d'ajustements amorcés à l'issue d'un désaccord entre les membres de la cellule de crise dans le cadre d'une injonction relative à une décision qui nécessite une acceptation collective. Il amène à une manipulation de la décision par réduction des potentialités de réponses de l'interlocuteur.

Le biais de confirmation :

il consiste à se focaliser exclusivement sur des éléments prédéfinis et à exclure de façon inconsciente, mais radicale des éléments en désaccord avec ces derniers.

Le biais rétrospectif :

il consiste à estimer, a posteriori, qu'un événement était probable ou prévisible, alors qu'il ne l'était pas a priori sur la base des informations alors disponibles.

Conclusion

Si les biais ne sont pas évitables, leur expression peut néanmoins être diminuée par une vigilance et une discipline collectives. Dans un contexte d'anxiété et d'incertitude, de surcharge informationnelle et cognitive et de surexpression des émotions, nous invitons sincèrement les cellules à s'organiser de manière à mieux objectiver leurs débats et, surtout, leurs prises de décision.

Raphaël De Vittoris

in

Raphaël de Vittoris est Group crisis manager de Michelin depuis 2015, il est aussi enseignant et chercheur en sciences de gestion sur les problématiques de gestion de crise, gestion des risques, communication de crise, négociation de crise et biais cognitifs en situation de crise. Docteur en sciences de gestion et qualifié maître de conférence, diplômé d'un master en physiologie en environnement extrême, d'un master en administration d'entreprise et d'un master en hygiène, sécurité et environnement, il enseigne dans divers masters et il est membre du board de l'Institut d'études des crises et d'intelligence économique et stratégique. Il est aussi l'auteur de « surmonter les crises (Dunod, 2021) » et de « par de la la résilience et l'antifragilité (Eska, 2022) »

Antifragile
crisis turning into success

antifragile.fr

C'est le moment quizz !

Saurez-vous reconnaître le bon biais cognitif ?

1- Quel biais cognitif consiste à accorder trop d'importance aux premières informations qui nous sont présentées ?

- a) Rétrospectif b) Confirmation c) Ancrage

2- Quel biais cognitif consiste à interpréter sélectivement les informations qui confirment nos croyances préexistantes ?

- a) Attribution b) Confirmation c) Narration

3- Quel biais cognitif consiste à attribuer des causes à des événements qui peuvent être dus à des facteurs externes ?

- a) Ancrage b) Attribution c) Représentativité

4- Quel biais cognitif consiste à penser que quelque chose est plus probable simplement parce qu'elle ressemble à nos idées préconçues ?

- a) Présomption b) Représentativité c) Survivant

5- Quel biais cognitif consiste à surévaluer l'importance de certaines informations qui attirent notre attention ?

- a) Narration b) Champion c) Ancrage

6- Quel biais cognitif consiste à considérer que les choses qui ont survécu à une épreuve sont nécessairement meilleures ou plus adaptées ?

- a) Survivant b) Champion c) Attribution

7- Quel biais cognitif consiste à reconstruire les événements passés en utilisant des informations présentes, ce qui peut altérer notre perception de la réalité ?

- a) Rétrospectif b) Représentativité c) Ancrage

8- Quel biais cognitif consiste à attribuer les résultats positifs à notre talent ou nos compétences, mais à blâmer les résultats négatifs sur des facteurs externes ?

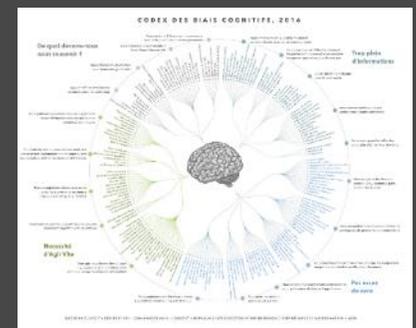
- a) Attribution b) Narration c) Survivant

 Réponses sur notre site Web
www.crise-resilience.com

PLUS D'INFO GRATUITES

Cliquez sur l'image pour accéder aux contenus

À Lire



À VOIR



Cliquez sur l'image pour accéder aux contenus

Pourquoi est-il possible de négocier lors de cyberattaque

La question est posée et, en fonction de l'interlocuteur qui répondra à celle-ci, la réponse variera peu.

Nous ne paierons pas.

Alignement conscient ou non sur les éléments de langage habituellement utilisés par les autorités, les entreprises et les entités qui font face, pourtant, à un dilemme particulier.

Face à une cyberattaque où le chantage existe, il convient de revenir aux fondamentaux de la gestion de crise et, en particulier, à un outil méconnu : **la négociation de crise.**



par Lilian Laugerat



Dirigeant du cabinet de conseils SOLACE
Expert en sûreté et en gestion de crise.
Négociateur.

Face à une cyberattaque où le chantage existe, il convient de revenir aux fondamentaux de la gestion de crise et, en particulier, à un outil méconnu : la négociation de crise.

En période de crise, la posture dérogatoire mobilisée se nomme la gestion de crise. Elle se caractérise par la mise en place d'une organisation dédiée composée d'une ou plusieurs cellules de crise.

Les attendus de cette organisation sont simples et clairs : gérer les impacts sur les personnes, les activités, l'image et la réputation, la responsabilité et, le cas échéant, l'environnement. Ce serait oublier la multitude de parties prenantes internes et externes impliquées dans la résolution, impactées de manière directe ou indirecte par l'attaque, à informer de la réalité de l'acte de malveillance.

Face à un acte de malveillance (une attaque cyber est, par définition, un acte de malveillance opéré par un ou plusieurs individus au sein d'une organisation constituée ou non dans le but d'atteindre un ou plusieurs objectifs), il existe plusieurs façons d'opérer et d'agir.

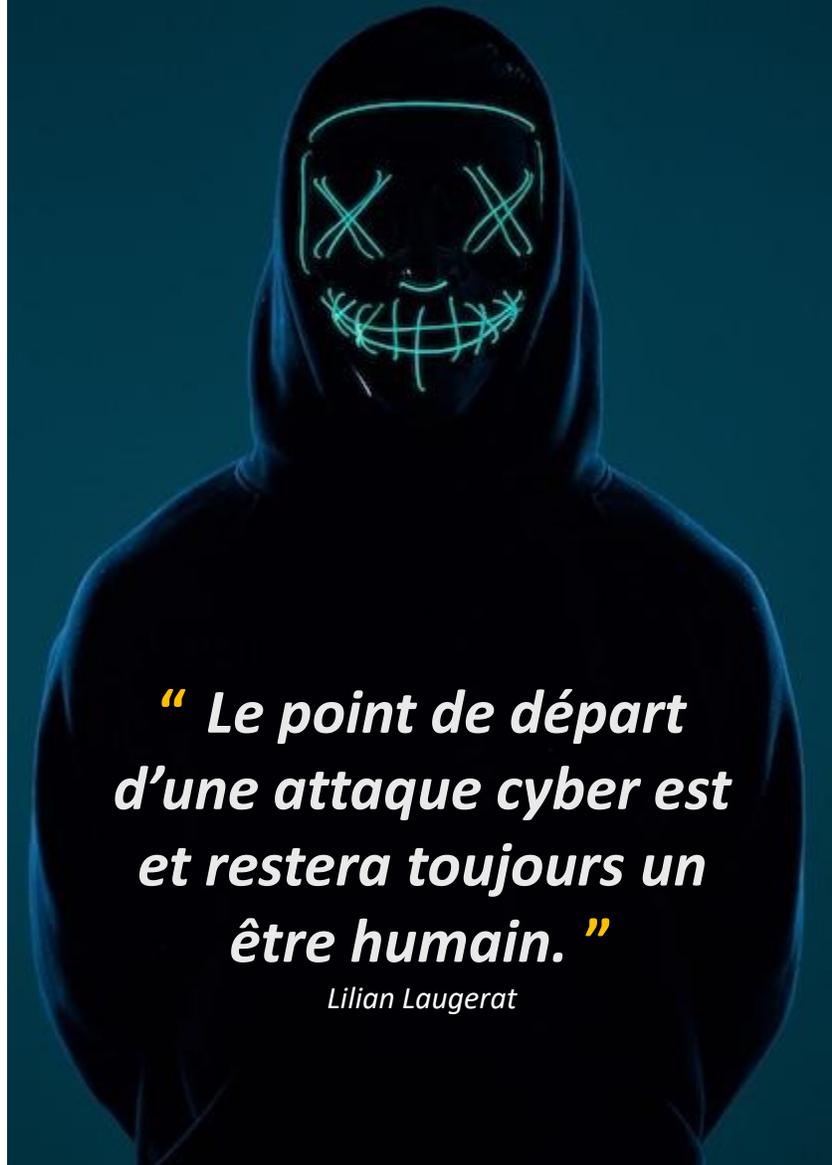
Une attaque cyber suit les mêmes grandes lignes que les modes opératoires des malveillants. Nous ajoutons bien entendu la dimension technique à cette attaque où la dimension humaine prend pourtant tout son sens. Le point de départ d'une attaque cyber est et restera toujours un être humain.

Celui qui appuiera sans hésiter sur la touche « Enter » pour lancer son attaque et attendre tranquillement la réaction de sa cible. Et la réaction de celle-ci est variée, variant de l'état de sidération à celui de déni, en passant ensuite par une vague d'émotions oscillant entre la colère et la peur des conséquences.

Cet attaquant sait également qu'en fonction de la cible visée et de son importance, les grands moyens vont être déployés pour minimiser les conséquences de son acte et essayer de lui faire commettre une erreur pour le repérer.

Il y a à ce jour une telle attractivité pour ce domaine qu'une littérature sans fin, des salons et des ateliers fleurissent de toute part, donnant à l'occasion un état des lieux de nos soi-disant forces et encore plus de nos faiblesses.

La négociation de crise n'est pas toujours invitée à la table de la gestion de crise cyber.



“ Le point de départ d'une attaque cyber est et restera toujours un être humain. ”

Lilian Laugerat

La négociation de crise n'est pas toujours invitée à la table de la gestion de crise cyber.

Sans doute, car la discipline est méconnue. Sans doute parce que, pour beaucoup, elle se borne à la prise en compte de la demande de rançon. Sans doute aussi parce que la ligne stratégique affichée est « nous ne paierons pas ». Sans doute, enfin, parce que beaucoup pensent savoir négocier face à un cyberattaquant.

Négocier en période de crise ne s'improvise pas.

C'est une véritable expertise associée obligatoirement à une éthique simple et directe : expliquer à un malveillant (quel qu'il soit) qu'il ne peut pas faire ou obtenir obligatoirement ce qu'il désire malgré le rapport de force installé au début de la période de crise.

Et cela dans un cadre où la confidentialité est la règle, où le silence médiatique est la clé.

Face à un acte de malveillance « cyberattaque », la gestion de crise ne peut seulement se résumer à une réponse technique.

Certes, celle-ci est importante dans la compréhension du périmètre affecté, voire infecté. Elle a pourtant des limites, car, même si l'attaquant laisse derrière lui quelques traces de son mode opératoire, la compréhension de son ou de ses objectifs n'est pas toujours prise en compte.

Négocier en période de gestion de crise revient à expliquer à l'autre (dans ce cas l'attaquant) qu'il ne peut pas faire obligatoirement ce qu'il veut et que, si un accord doit intervenir, celui-ci s'effectuera selon certaines modalités.

La négociation de crise entre de plain-pied dans la partie communication. Il ne s'agit ni de la communication de crise vers les médias ni de la communication en période de crise vers les parties prenantes touchées.

C'est un véritable moyen de créer un lien avec l'origine de l'attaque et d'en comprendre les objectifs. Négocier, c'est avant tout échanger, et pas seulement sur le montant de la rançon.

La vraie difficulté sera alors de décrypter le contenu des échanges. En effet, pas de son de voix, que des mots écrits de manière mécanique avec peu d'émotions palpables. Une sorte de monstre froid avec lequel il faudra pourtant dialoguer (le dialogue fait également partie de la négociation) tout en cherchant à comprendre quelles sont alors les véritables intentions.

Décrypter cet ensemble ne s'improvise pas.

Comprendre un auteur d'acte de malveillance demande une ouverture d'esprit particulière et une acceptation complète d'une situation inédite.

Ne pas mobiliser une compétence de négociation de crise dès le début d'une cyberattaque réduit une partie du champ des possibles. Ne surtout pas croire que la négociation de crise pourra tout résoudre. Comme toute discipline liée à la gestion de l'humain, c'est la perfection de l'imperfection.

La mobilisation de cette expertise permet, dans une grande majorité des cas, d'ajouter une variable supplémentaire à l'équation de gestion, voire de résolution de la crise.

S'improviser négociateur entre dans le registre de la faute à éviter. Elle décrédibilise la fonction et les futures possibilités offertes.

Négocier en silo en oubliant les principes de la gestion de crise est également une erreur à éviter.

La négociation de crise s'inscrit donc véritablement dans la stratégie de gestion d'une crise cyber. Elle apparaît comme une option à l'instar de toutes les autres disciplines entrant dans le champ de la résolution ou, tout du moins, dans la gestion des multiples impacts et dans la communication vers les parties prenantes.

En d'autres mots, ne pas l'intégrer, c'est déjà créer un décalage dans la réponse à apporter.

Lilian Laugerat

Négocier, c'est avant tout échanger, et pas seulement sur le montant de la rançon.



LES POINTS CLÉS DE L'INTÉGRATION DE LA NÉGOCIATION EN PÉRIODE DE CRISE CYBER

Intégrer le négociateur ou l'équipe de négociation au sein du dispositif de gestion de crise dès le constat de la réalité de la cyberattaque.

Intégrer la négociation de crise au sein de la stratégie globale et non pas seulement comme un moyen pour négocier le montant d'une éventuelle rançon.

Préparer les hypothèses de travail en prenant en compte la totalité des impacts et les attentes de toutes les parties prenantes.

Valider les options favorables et défavorables avant d'engager une négociation avec le point de contact proposé.



Lilian Laugerat est un expert en sûreté et en gestion de crise. Il dirige le cabinet de conseils SOLACE, spécialisé dans l'analyse des risques sûreté et la posture de gestion de crise. Solace est une entité de Cecys Group, filiale du Groupe Goron. Lilian LAUGERAT a une expérience opérationnelle dans le domaine du renseignement et des interventions en zones sensibles. Il a été membre du Groupe d'Intervention de la Gendarmerie Nationale (GIGN) de 2000 à 2006, où il a occupé en particulier les fonctions de chef de la cellule de négociation de crise Il a également été instructeur OACI (Organisation de l'aviation civile internationale) pour la formation des négociateurs de crise à travers le monde.



lilian.laugerat@solace.fr



solace.fr

Soyez prêt à affronter toute crise qui pourrait menacer votre entreprise

Survivez à la prochaine crise !

Initier votre Gestion de CYBERCRISE
En 5 demi-journées pratiques

INCLUS DANS CE BOOTCAMP

- + de 20 heures de cours incluant 12 ateliers de mise en pratique
- 20 gabarits prêts à l'emploi pour gagner un temps précieux
- 5 heures de coaching privé pour vous accompagner
- 3 conférences privées en complément de la formation
- 10 affiches de sensibilisation personnalisables
- Accès à vie à la formation et aux mises à jour
- Accès à vie au Club privé Crise&Résilience

Atelier pratique basé sur les normes ISO 22301 et ISO 22361

Taux de satisfaction 96%

Date de la formation
📅 23 au 26 mai 2023
8h à 12h (Québec) ou 13h à 17h (France)

Prix de vente public
~~2 997 \$~~
2 497 \$ + taxes

Valeur du Bootcamp +bonus équivaut à 14 000\$

Maintenez vos activités lors du prochain black-out !

Préparer votre Plan de Continuité des Affaires
En 6 demi-journées

INCLUS DANS CE BOOTCAMP

- + de 20 heures de cours avec exercices pratiques
- 10 gabarits prêts à l'emploi pour gagner un temps précieux
- 5 heures de coaching privé pour vous accompagner
- 10 affiches de sensibilisation personnalisables
- Accès à vie à la formation et aux mises à jour
- Accès à vie au Club privé Crise&Résilience

Formation basée sur la norme ISO 22301

Taux de satisfaction 95%

Formation en ligne

Prix de vente public
~~2 997 \$~~
2 497 \$ + taxes

Valeur total de la formation + bonus est supérieure à 10 000\$

PROFITEZ 500\$ de réduction jusqu'au 30 avril 2023

Inscrivez-vous dès maintenant à nos formations pour protéger votre business contre les menaces.

www.crise-resilience.com/formation

Le management d'opportunités face aux nouvelles crise



Toutes les origines des grandes crises suivent une triangulation influente entre les parties financière, sociale et économique.

Avec l'évolution technonumérique, cela nous amène à un autre type d'influence incorporant le facteur information.

Les futurs modèles de management des opportunités issus de ces crises devront être mieux pensés, pragmatiques et organisationnels.

par **Christophe Saussereau**



Dirigeant du cabinet EIS/SAUSSEREAU
Spécialiste en développement commercial par
intégration de solutions IT



Toutes les origines des grandes crises suivent une triangulation influente entre les parties financière, sociale et économique. Avec l'évolution technonumérique, cela nous amène à un autre type d'influence incorporant le facteur information. Les futurs modèles de management des opportunités issus de ces crises devront être mieux pensés, pragmatiques et organisationnels.

Profil

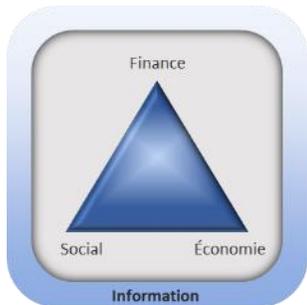
Les grandes crises dans les pays industrialisés présentent de grandes différences. En effet, l'environnement institutionnel, technologique et international a fortement évolué depuis plus d'un siècle. Ces crises passées ont provoqué des perturbations fortes et durables dans les sociétés industrielles et sur les opportunités ciblées.

L'évolution de ces principaux facteurs de crise systémique ayant eu un impact socioéconomique :

- L'ouverture et la libération des marchés;
- L'augmentation de la concurrence avec les pays émergents (BRICS), qui produisent à faible coût;
- Les limites d'un système financier et spéculatif non maîtrisé;
- L'excès d'investissement/de production par rapport à la demande;
- L'augmentation d'une faille sociale et, par conséquent, économique;
- L'influence des pouvoirs politiques dans les organisations.
- Pour chaque facteur, il y a eu une opportunité de développement

Les différentes crises ont fait émerger des entreprises innovantes qui ont su en profiter

Bien avant l'ouverture des marchés et de la concurrence, la plupart des opportunités se développaient lors de crises, autour de trois axes (financier, social et économique).



Ensuite, l'arrivée de la mondialisation à grande échelle a permis d'accélérer le paramètre « information ».

Les crises modernes ont fait apparaître une révolution et une évolution dans les systèmes de gestion de l'information et de communication, et elles ont fait émerger de nouvelles méthodologies de travail.

De nos jours, sans informations certifiées en temps réel, il est difficile de pouvoir piloter sereinement son activité et de mesurer les conséquences à la fois dans les risques et dans les opportunités



L'importance des systèmes d'information afin de mieux gérer les opportunités

De nos jours, sans informations certifiées en temps réel, il est difficile de pouvoir piloter sereinement son activité et de mesurer les conséquences à la fois dans les risques et dans les opportunités (la fiabilité des sources, la préservation des données dans son environnement).

Les nouvelles applications de gestion d'entreprise (ERP, CRM, business intelligence, etc.) sont devenues de véritables outils de pilotage.

ERP : PGI (progiciel de gestion intégré). **CRM** : GRC (Gestion de la relation client)
Business Intelligence : veille économique, veille stratégique ou informatique décisionnelle.

Savoir décoller est une chose, savoir atterrir sans dommage en est une autre

En effet, pour chaque crise, devenue de plus en plus complexe avec le temps, c'est de savoir prévoir longtemps, d'avoir tous les atouts nécessaires – et au-delà – afin de la surmonter rapidement et efficacement avec un véritable plan de continuité et de reprise de l'activité de l'entreprise. Plus qu'une opportunité, il s'agit d'une nécessité vitale à la survie d'une entreprise.

Les moindres défauts peuvent devenir sources d'une crise : problèmes financiers (trésorerie, besoin de fonds de roulement, fonds de roulement, etc.), défauts liés à l'innovation et à la qualité d'un produit ou d'un service, mauvaise gestion du personnel, mauvaise gestion prévisionnelle, manque de suivi clients, méconnaissance des marchés, etc. Les signaux peuvent être verts un jour et devenir rapidement rouges le lendemain. Les causes sont multiples et bien souvent dues à une mauvaise gestion des ressources et du temps et à des décisions non maîtrisées à moyen et long terme.

Seules les entreprises ayant la bonne formation sauront gérer l'information et l'appliquer efficacement.

PISTES DE RÉFLEXION POUR SAISIR LES OPPORTUNITÉS

Le management des opportunités : une autre façon d'aborder la partie organisationnelle et sociale en entreprise – Exemple dans l'industrie

Lors de la crise qui a débuté en France en 2008, les secteurs de la finance et de l'industrie et le secteur social sont tombés; la plupart des entreprises ont dû fermer et placer leurs collaborateurs au chômage partiel. La question que nous nous sommes posée était assez pragmatique : comment préserver son activité, pouvoir dégager des bénéfices, lorsque la situation socioéconomique et financière est négative?

Le principal objectif était de ne pas investir, d'utiliser efficacement ce que nous avons déjà en notre possession (humain et matériel).

La création d'un système matriciel managérial des opportunités à la fois collaboratif et participatif, à travers un système d'information par des validations simples, a été un véritable défi. Nous devons changer complètement le modèle managérial et organisationnel de l'entreprise en nous tournant vers un modèle de gestion neuronale dans les choix et décision rapide.

L'entreprise 202X, une ressource à surveiller en temps réel

L'information est devenue un facteur clé dans les choix stratégiques d'une entreprise. La constante évolution de l'information fait en sorte que la prise de décision doit se faire selon des critères précis, maîtrisables et contrôlables en temps réel.

De nos jours, l'outil de production par la maîtrise financière (énergie, matière première, etc.) est de pouvoir disposer en temps réel de coûts complets de production qui évoluent automatiquement.

C'est une base indispensable afin de pouvoir développer une vraie stratégie en prenant en compte l'exacte situation de l'entreprise.

Savoir prendre les bonnes décisions qui s'imposent

Il est indispensable de disposer en temps réel des résultats nets avant impôts détaillés par période, produit, client et secteur et de pouvoir simuler l'impact de toutes les décisions envisagées (commerciales, organisationnelles, relatives aux investissements, etc.) afin de connaître préalablement l'incidence qu'elles auraient sur les résultats.

Le management des opportunités est géré en interne

Ce management se trouve essentiellement dans sa propre organisation : amélioration de la gestion financière en temps réel, de la sécurisation du système d'information et de la révision de son management opérationnel (humain, performance commerciale, amélioration de la rentabilité des unités de production, etc.) et externe (gestion de l'information auprès de ses clients, fournisseurs, réseaux professionnels, etc.).

Ce système de management des opportunités est un véritable pilotage opérationnel tout en étant participatif et collaboratif. Il est possible, à partir du moment où la gouvernance de l'entreprise accepte l'idée du changement de modèle managérial, d'assurer son propre audit en interne afin de détecter les moindres signes de faiblesse, d'accepter de les corriger et de veiller à rendre ces corrections pérennes et fiables.

L'opportunité numérique durant la crise sanitaire

Autre point, la crise sanitaire de 2019, qui a permis à l'ensemble du monde numérique de faire une belle croissance. Le télétravail, le commerce électronique, la communication, etc., ont permis de développer sans souci diverses opportunités durant cette période d'inactivité pour certains et d'activité intenses pour d'autres.

L'émergence de ces opportunités a aussi révélé une grande part de négligence dont les Pirates informatiques ont su profiter pleinement à travers les failles dans les organisations et les systèmes d'information non maîtrisés. La plupart du temps, les décisions furent précipitées et non réfléchies.

Un cycle infoéconomique profitable à ceux et celles qui détiennent le bon usage de cette opportunité.

Analyser les marchés et les choix socioéconomiques et financiers, détecter la bonne information et s'attacher aux actions les plus influentes et pas forcément les plus importantes dans une organisation permettront d'obtenir de véritables opportunités.

Les marchés évoluent en permanence dans un brouillard perpétuel d'informations de toute origine. Chaque prise de décision ne doit pas être l'unique solution, mais résulter d'une multitude de possibilités pour sortir d'une crise. Le plus important n'est pas forcément de maintenir son cap, mais surtout de ne pas perdre de vue ses objectifs et d'être irréprochable.

Christophe Saussereau



Christophe Saussereau De la recherche appliquée au développement des systèmes d'information, un parcours dans divers secteurs d'activité à l'international. Mon activité s'oriente principalement vers les développements de systèmes d'information (gestion financière, sécurité et conseil etc.) et de les transmettre à travers des formations en entreprise et des écoles de commerce.



cabineteis@gmail.com

Simulez en **3D** votre prochaine cyberattaque!

Plongez dans
l'univers
des crises
avec notre
simulation
immersive.



Téléchargez gratuitement
5 idées de scénarios de
gestion de crise



Nous offrons GRATUITEMENT 1h de simulation de crise.

Attention le nombre de places est limité!

Nous contacter ici : <https://www.crise-resilience.com/simulation>

La crise ne frappe pas avant d'entrée!

6 raisons d'effectuer des exercices de gestion de crise



Les crises sont comme les examens surprises, on ne sait jamais quand elles vont arriver, mais on peut être sûr qu'elles vont nous mettre à rude épreuve!

Que ce soit des catastrophes naturelles, des pannes techniques, des cyberattaques, des erreurs humaines ou tout autre événement imprévu, **la gestion de crise est absolument essentielle.**

Par Karine Maréchal-Richard 

Experte en continuité des affaires et gestion de crise
Consultante, formatrice et conférencière dans les domaines de la continuité des affaires et de la gestion de crise depuis 15 ans.



Les crises sont comme les examens surprises – on ne sait jamais quand elles vont arriver, mais on peut être sûr qu’elles vont nous mettre à rude épreuve!

Que ce soit des catastrophes naturelles, des pannes techniques, des cyberattaques, des erreurs humaines ou tout autre événement imprévu, la gestion de crise est absolument essentielle.

Parce que perdre nos précieux biens et actifs ou laisser les perturbations affecter nos opérations n’est pas une option envisageable. Et, bien sûr, pour être prêt à faire face à de telles situations, il est nécessaire de s’entraîner.

Et quoi de mieux que des exercices de gestion de crise pour cela?

C’est l’occasion idéale de simuler une crise réelle, mais à la manière d’un jeu de rôle, afin de tester et de savoir si tout le monde est capable de résoudre des problèmes complexes dans un environnement stressant.

Voici six raisons pour lesquelles les exercices de gestion de crise sont nécessaires.

1-Évaluer ses plans, ses processus et ses procédures :

Les exercices de gestion de crise permettent de tester et de vérifier l’efficacité de tous les plans utiles en situation de crise tels que le plan de communication de crise, le plan de reprise informatique, le processus de détection des événements, l’arbre d’appel, la procédure d’activation des cellules de crise, et bien d’autres encore.

En les testant, on peut détecter les vulnérabilités et les corriger avant qu’une véritable crise ne se produise.

Cela permet de s’assurer que les plans sont solides et que les processus sont bien rodés en cas de crise, ce qui est essentiel pour minimiser les impacts d’une crise et pour une reprise rapide des activités.

2-Tester la salle de crise :

Les exercices de gestion de crise permettent de tester tous les équipements nécessaires à la salle de crise et de s’assurer qu’ils sont fonctionnels et prêts à être utilisés en cas de crise réelle. Les équipements essentiels comprennent notamment les radios, les téléphones, les imprimantes locales, le système de vidéoconférence, les ordinateurs, une télévision, des tableaux blancs et d’autres équipements spécialisés qui pourraient être nécessaires pour gérer la crise.

La salle de crise est un endroit qui sert de centre de coordination pour l’équipe de gestion de crise. Par sa fonctionnalité, il est crucial de s’assurer que la salle dispose de tout ce dont l’équipe a besoin pour travailler de manière efficace.

“ Mieux vaut se planter en simulation de crise que lors d’une crise réelle! ”

Alexandre Fournier

Les exercices de simulation permettent de tester la salle de crise en termes de fonctionnalité et de convivialité.

Ils permettent également de vérifier si la salle de crise est suffisamment grande pour accueillir tous les membres de l’équipe de gestion de crise ainsi que les parties prenantes externes qui pourraient être nécessaires pour aider à gérer la crise.



3-Connaître son rôle et ses responsabilités :

En situation de crise, il est important de savoir qui est responsable de quoi et qui fait quoi.

Les exercices sont donc une excellente opportunité pour les différents acteurs impliqués de comprendre leur rôle et leurs responsabilités en cas de crise. Cela peut inclure les membres de l’équipe de crise, les dirigeants de l’entreprise, les employés et les partenaires externes.

En simulant une crise, chaque personne est en mesure de mieux comprendre ses tâches et ses responsabilités, ainsi que celles des autres membres de l’équipe.

Cela permet à chacun de savoir qui contacter en cas de besoin, à qui rendre compte et comment collaborer avec les autres pour résoudre la crise.

4-Améliorer la coordination :

Lors d'une crise, il est essentiel que tous les acteurs clés d'une gestion de crise travaillent ensemble de manière coordonnée pour résoudre un problème.

Les exercices permettent de mettre à l'épreuve la coordination entre les membres de l'équipe de crise et d'identifier les éventuels problèmes de communication, de prise de décision, de gestion des ressources et d'organisation des équipes.

En simulant une crise, les équipes peuvent s'entraîner à travailler ensemble de manière efficace et développer une meilleure compréhension des rôles et des responsabilités de chacun dans la gestion d'une crise.

5-Apprendre à se connaître en période de stress aigu :

Les exercices de gestion de crise sont bien plus que de simples simulations. Ils offrent une opportunité unique de découvrir de nouvelles compétences et de mieux se connaître en situation de crise.

En effet, lors d'une crise, le stress peut prendre le dessus et perturber notre comportement habituel.

Les exercices permettent ainsi de développer de nouvelles compétences en gestion de stress, en communication sous pression, en résolution de problèmes complexes et en prise de décisions rapides.

En les pratiquant régulièrement, les membres de l'équipe de crise peuvent mieux comprendre leurs propres réactions en situation de crise et apprendre à les contrôler pour être plus efficaces.

Les exercices permettent également d'identifier les membres de l'équipe qui sont particulièrement doués dans certains rôles de la gestion de crise, ce qui permet de mieux répartir les responsabilités et de maximiser les chances de succès en cas d'urgence.

6-Renforcer la confiance :

En effectuant des exercices de simulation, les membres de l'équipe peuvent être plus confiants en leur capacité à réagir rapidement et efficacement en cas de crise.

Ces exercices peuvent également renforcer leur confiance dans l'organisation en sachant que des plans de gestion de crise appropriés ont été élaborés et que les membres de l'équipe ont été correctement formés.

En travaillant ensemble pour résoudre des scénarios de crise simulés, les membres de l'équipe peuvent renforcer leur cohésion et leur confiance les uns envers les autres.

Cela peut créer un sentiment de confiance mutuelle, qui peut être précieux lorsqu'il s'agit de travailler ensemble dans des situations d'urgence réelles.





“ Les exercices aident à renforcer la confiance de l'équipe, à améliorer la cohésion et l'engagement envers l'organisation.”

Karine Maréchal-Richard

La confiance accrue peut également renforcer la motivation de l'équipe et son engagement envers l'organisation, car elle se sent préparée à gérer toute situation qui pourrait survenir.

La confiance est un élément crucial dans la gestion de crise, car elle permet aux membres de l'équipe de rester calmes et de prendre des décisions rapides et réfléchies en cas d'urgence.

Les exercices de gestion de crise peuvent jouer un rôle important dans le renforcement de cette confiance, en donnant aux membres de l'équipe les compétences, les connaissances et l'expérience nécessaires pour faire face à toute situation de crise qui pourrait se présenter.

Vous l'aurez compris, les crises ne frappent pas au portes et peuvent survenir à tout moment, et les exercices permettent aux équipes de se préparer en testant les plans de gestion de crise, la salle de crise, les rôles et responsabilités, la coordination entre les membres de l'équipe, et en développant des compétences en gestion de stress et en prise de décision rapide.

Les exercices aident également à renforcer la confiance de l'équipe, à améliorer la cohésion et l'engagement envers l'organisation, et à minimiser les impacts d'une crise en permettant une reprise rapide des activités.

En somme, les exercices de gestion de crise sont un investissement essentiel pour la préparation et la résilience des entreprises et des organisations face aux crises imprévues.



Karine Maréchal-Richard

Simulez en **3D**
votre prochaine
cyberattaque!

Plongez dans
l'univers
des crises
avec notre
simulation
immersive.



**Nous offrons GRATUITEMENT
1h de simulation de crise.**

ATTENTION NOMBRE DE PLACES LIMITÉ!

Nous contacter ici :

<https://www.crise-resilience.com/simulation>

Téléchargez gratuitement
5 idées de scénarios de
gestion de crise



16 SECRETS D'UN EXERCICE DE GESTION DE CRISE RÉUSSI

1. Choisissez le type et le thème de votre exercice :

Le type et le thème de votre exercice doivent être choisis en fonction de l'objectif que vous souhaitez atteindre. L'exercice de table est une discussion structurée visant à valider les plans et les procédures élaborés pour gérer une crise, alors que la simulation offre une expérience immersive d'une situation de crise fictive aux participants.

2. Définissez la durée et le moment auquel vous voulez réaliser votre exercice :

un jour de semaine, un soir, un jour férié, en pleine nuit, en pleine période estivale, etc. La durée et le moment de votre exercice doivent être définis en fonction des contraintes de votre organisation et de vos participants. Il est important de choisir un moment où les participants peuvent se concentrer sur l'exercice sans perturber les activités normales de l'organisation.

3. Constituez un comité de préparation composé d'experts pour concevoir un scénario réaliste.

Le comité de préparation doit être composé d'experts ayant une connaissance approfondie de votre organisation et de la crise que vous souhaitez simuler. Ils doivent travailler ensemble pour concevoir un scénario réaliste et pertinent.

4. Assurez-vous que tous les participants sont formés et informés sur les procédures à suivre en cas de crise.

Afin de garantir une réponse adéquate et coordonnée lors d'une crise, il est crucial que chaque acteur clé comprenne son rôle et ses responsabilités, le fonctionnement des cellules de crise décisionnelle et opérationnelle, ainsi que les outils élaborés pour gérer une crise.

5. Planifiez la date de l'exercice.

La date de l'exercice doit être planifiée en fonction des contraintes de votre organisation et de vos participants, en prenant en compte les événements externes qui pourraient perturber l'exercice.

6. Définissez clairement le périmètre et assurez-vous que votre exercice n'impactera pas le quotidien.

Le périmètre de l'exercice doit être clairement défini pour éviter tout impact négatif sur les activités normales de l'organisation. Une fois le périmètre défini, vous pourrez identifier les participants à l'exercice.

7. Identifiez les participants à l'exercice (membres de la cellule de crise décisionnelle, opérationnelle, les partenaires, observateurs, etc.).

Les participants à l'exercice doivent être sélectionnés en fonction de leur rôle dans la gestion de crise. Cela peut inclure les membres des cellules de crise décisionnelle et opérationnelle, ainsi que des partenaires externes, parmi d'autres. Les observateurs jouent un rôle crucial, car ils suivent le déroulement de l'exercice, identifient les domaines d'amélioration et apportent des retours constructifs après l'exercice. Les observateurs peuvent être des membres de l'organisation non directement impliqués dans la réponse à la crise, ou bien des experts externes en gestion de crise.

8. Déterminez les objectifs de l'exercice.

Les objectifs de l'exercice doivent être déterminés en fonction des résultats attendus et des domaines à tester. Ils doivent être clairement communiqués à tous les participants.





9. **Définissez votre scénario d'exercice en tenant compte de la maturité de votre organisation.** Le scénario d'exercice doit être défini en tenant compte de la maturité de votre organisation et des risques réels auxquels elle est confrontée. Il doit être réaliste et pertinent.
10. **Construisez de fausses pièces pour rendre le scénario de crise le plus réaliste en faisant appel aux experts du domaine (liste des applications essentielles, fiches techniques, coupures de presse, faux courriels, extraits de médias sociaux, etc.).** Les fausses pièces doivent être construites pour rendre le scénario de crise le plus réaliste possible. Les experts du domaine peuvent aider à créer des documents tels que des listes d'applications essentielles, des fiches techniques, des coupures de presse, des faux courriels, des extraits de médias sociaux, etc.
11. **Introduisez des stimuli pour rythmer votre exercice (appel téléphonique d'un journaliste, une prise d'otage, un faux spécialiste TI, réaction d'un partenaire, etc.).** Les stimuli doivent être introduits pour rythmer l'exercice et simuler les réactions réelles. Des collaborateurs peuvent jouer des rôles pour augmenter le réalisme de l'exercice.
12. **Produisez votre chronogramme qui présentera toute la chronologie de votre exercice.** Un chronogramme détaillé est essentiel pour assurer le bon déroulement de l'exercice de gestion de crise. Il permettra à l'animateur de l'exercice de suivre la
13. **Prévoyez la logistique de l'exercice : la préparation de la salle, les déplacements, les repas, etc.** La logistique de l'exercice doit être prévue pour garantir un déroulement efficace de l'exercice.
14. **Répétez avec le comité de préparation pour vous assurer que tout est en place.** Pour garantir que tout est prêt et s'enchaîne harmonieusement, une séance de répétition avec le comité de préparation doit être organisée. Elle permet de s'assurer que tous les éléments sont en place et que les transitions se déroulent sans problème.
15. **Préparez les documents qui vous permettront de réaliser un retour d'expérience.** Pour faciliter l'analyse de l'exercice et la mise en place de mesures d'amélioration, vous pouvez préparer à l'avance les questions qui vous permettront de réaliser votre retour d'expérience.
16. **Gagnez en rapidité en préparant certaines parties du bilan d'exercice.** Afin de gagner du temps lors de la rédaction du bilan d'exercice, certaines parties peuvent être préremplies, telles que la liste des participants, le scénario de l'exercice, les objectifs et le chronogramme, présentés sous format Excel.

La chaîne d'approvisionnement

Les chaînes d'approvisionnement sont la colonne vertébrale de l'économie mondiale, mais leur fragilité peut entraîner des conséquences catastrophiques.

Découvrez les enjeux et les solutions pour renforcer leur résilience.

par **Alexandre Fournier**



Expert en gestion et simulation de crise

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



Les entreprises et les consommateurs dépendent de manière cruciale de l'approvisionnement en matières premières, en pièces détachées et en produits finis, et cette chaîne d'approvisionnement complexe, multiforme et mondialisée implique un ensemble d'acteurs, tels que les fournisseurs, les transporteurs, les distributeurs et les prestataires de services. Les enjeux liés à cette chaîne sont nombreux, allant de l'optimisation des coûts et des délais à la qualité et à la sécurité des produits ainsi qu'à la traçabilité des flux.

Cependant, la chaîne d'approvisionnement n'est pas sans risques. Les interruptions peuvent être causées par des événements imprévus tels que des conflits sociaux, des guerres, des catastrophes naturelles, des pandémies ou des cyberattaques, ainsi que par des facteurs économiques ou politiques locaux ou mondiaux.

Ces interruptions peuvent avoir des conséquences dramatiques pour les entreprises, les consommateurs, l'économie et le pays dans son ensemble, entraînant des pertes financières, des perturbations dans la production et la distribution, ainsi qu'une pénurie de produits ou services essentiels.

“ Ensemble lié de ressources et de processus qui commence avec l'identification de l'origine des matières premières et qui va jusqu'à la livraison des produits ou services à l'utilisateur final en passant par les divers modes de transport ”

*Définition de la chaîne d'approvisionnement
Norme ISO 28000*

DE L'APPROVISIONNEMENT À LA LIVRAISON

La chaîne d'approvisionnement est l'ensemble des activités qui visent à fournir un produit ou un service, de la matière première à la livraison au client.

Pour que cette chaîne soit efficace, il est important de bien gérer les différents types de flux qui la composent. Une bonne gestion de ces flux permet d'optimiser les coûts, de réduire les délais de livraison et d'assurer une meilleure satisfaction client.

Voici les trois principaux flux.

Les flux physiques constituent le mouvement des produits et des matières premières tout au long de la chaîne d'approvisionnement. Les fonctions d'approvisionnement, de gestion des stocks, d'entrepôt et de transport sont toutes des éléments clés de la gestion des flux physiques. L'objectif ultime de la gestion des flux physiques est de livrer les bons produits, au bon endroit, au bon moment, dans les bonnes quantités et en bon état, tout en minimisant les coûts. Pour y parvenir, il est important de maintenir une visibilité sur l'ensemble de la chaîne d'approvisionnement, de surveiller les niveaux de stock et de gérer les délais de livraison.

Les flux d'information sont également essentiels pour la gestion de la chaîne d'approvisionnement. En effet, les informations sont nécessaires pour planifier les opérations de la chaîne, pour prendre des décisions éclairées et pour suivre les performances. Les flux d'information sont souvent associés aux mégadonnées (big data), car les entreprises génèrent et stockent une grande quantité de données tout au long de la chaîne. Ces données comprennent l'historique des ventes et des mouvements, les différents intervenants du processus, les stratégies adoptées, les moyens mis à disposition et les indicateurs de performance. Les informations sur les prix (des marchandises, du transport et des prestations effectuées par les prestataires d'une entreprise) sont également répertoriées dans la base de données. Les entreprises doivent être en mesure de faciliter l'accès à ces informations, en utilisant des logiciels de gestion de données performants, afin d'améliorer la transparence et la collaboration au sein de la chaîne d'approvisionnement.

Les flux financiers sont les mouvements de trésorerie tout au long de la chaîne d'approvisionnement. Ils comprennent toutes les activités qui se rapportent au traitement des commandes, au contrôle du calendrier des livraisons, des commandes et des paiements, ainsi qu'à la production de rapports de gestion. Les entreprises doivent être en mesure de surveiller et de gérer les flux financiers de manière proactive pour minimiser les risques de retards de paiement et de problèmes de trésorerie. Par exemple, un retard de facturation peut entraîner des conséquences sur la planification de l'approvisionnement, ce qui aura certainement un impact indirect sur la gestion des stocks et la trésorerie.



FONCTIONNEMENT DE LA CHAÎNE D'APPROVISIONNEMENT

Le fonctionnement de la chaîne d'approvisionnement peut varier en fonction de l'entreprise et du secteur d'activité, mais, en général, elle est constituée de plusieurs maillons :

- **Les fournisseurs**, qui sont les premiers maillons de la chaîne. Ils fournissent les matières premières, les pièces détachées ou les produits finis aux entreprises.
- **Les transporteurs**, qui sont responsables du transport de ces produits, du fournisseur à l'entreprise ou du stock à la plateforme de distribution.
- **Les distributeurs**, comme les grossistes ou les détaillants, qui assurent la vente des produits finis aux consommateurs finaux.
- **Les prestataires de services**, tels que les consultants ou les entreprises de logistique, qui peuvent également jouer un rôle dans la chaîne d'approvisionnement.

Chaque maillon de la chaîne est interdépendant et joue un rôle crucial dans son bon fonctionnement.

Les interruptions peuvent affecter différents types d'entreprises.

VOICI 3 EXEMPLES D'IMPACT DE RUPTURE

Secteur alimentaire :

L'exemple d'une usine de produits alimentaires qui utilise des matières premières telles que des ingrédients, des emballages et des étiquettes provenant de différents fournisseurs. Une fois les matières premières reçues, l'entreprise fabrique ses produits et les stocke dans son entrepôt. Lorsqu'une commande est passée, l'entreprise prépare l'envoi et fait appel à un transporteur pour livrer les produits au client final. Les interruptions dans la chaîne d'approvisionnement, telles que les retards de livraison de matières premières ou les problèmes de transport, entraîneront des retards de livraison et des pertes financières pour l'entreprise.

Secteur du service :

Dans le cas du service à la personne, par exemple une entreprise de nettoyage, on peut utiliser des équipements comme des aspirateurs, des produits de nettoyage et des uniformes fournis par différents fournisseurs. Lorsqu'un client passe une commande pour des services de nettoyage, l'entreprise planifie et alloue les ressources nécessaires pour effectuer le travail. Une interruption dans la chaîne d'approvisionnement pourra entraîner des perturbations dans la fourniture des services et impacter la satisfaction client.

Secteur médical :

Enfin, dans le secteur médical, une interruption de la chaîne d'approvisionnement peut être catastrophique. Prenons l'exemple d'une entreprise pharmaceutique qui produit des médicaments. Cette entreprise a besoin de matières premières telles que des principes actifs, des excipients et des emballages provenant de différents fournisseurs qui se trouvent hors de son pays. Une fois les matières premières en sa possession, l'entreprise produit les médicaments, les stocke et les distribue aux pharmacies et aux hôpitaux. L'interruption de la chaîne d'approvisionnement dans le domaine médical entraîne des pénuries de médicaments, qui mettront en danger la vie des patients.



DÉPENDANCE AUX APPROVISIONNEMENTS MONDIAUX

La mondialisation des échanges a favorisé une interdépendance croissante des économies à travers le monde, conduisant à une augmentation importante des approvisionnements mondiaux.

Aujourd'hui, de nombreuses entreprises dépendent au quotidien de la chaîne d'approvisionnement mondiale pour fournir les matières premières, les pièces détachées et les produits finis nécessaires à leur production.

Cette dépendance aux approvisionnements mondiaux présente des avantages tels que la diversification des fournisseurs, la réduction des coûts, l'optimisation des délais de production et une plus grande accessibilité des produits pour les consommateurs.

Cependant, cela présente également des inconvénients comme la fragilisation de la chaîne d'approvisionnement en cas de perturbations cyber, logistiques, économiques, politiques ou environnementales.

La mondialisation a un impact considérable sur certains secteurs économiques, qui sont fortement tributaires des approvisionnements à l'échelle mondiale.

Par exemple, l'industrie électronique est très dépendante de la chaîne d'approvisionnement mondiale pour les matières premières et les composants électroniques, qui sont souvent produits dans des pays en développement où les coûts de production sont moindres. Toutefois, cela rend cette industrie également vulnérable aux perturbations économiques et politiques dans ces pays.

Durant la pandémie, des centaines d'usines de production ont été à l'arrêt pendant plusieurs mois, entraînant une pénurie de pièces électroniques, ce qui a eu un impact sur l'industrie automobile à l'échelle mondiale.

De même, l'industrie automobile est dépendante de la chaîne d'approvisionnement mondiale pour les pièces détachées et les composants, ce qui la rend vulnérable à la fluctuation des prix et des coûts de transport, étant donné que les constructeurs automobiles externalisent souvent la production de certaines pièces détachées.

L'obstruction du canal de Suez en 2021, qui a eu des répercussions sur l'ensemble des ports et des bateaux bloqués à travers le monde, en est un exemple marquant.



CHAÎNE D'APPROVISIONNEMENT SUR LES BESOINS ESSENTIELS

Le gouvernement, les entreprises et les citoyens sont tous dépendants de produits provenant de l'étranger, qu'ils soient matériels ou non. Cependant, la pandémie de COVID-19 et la crise énergétique avec la Russie ont mis en évidence les risques d'une forte dépendance aux importations et aux chaînes d'approvisionnement fragiles. Tout ralentissement ou interruption dans ces chaînes peut avoir des conséquences graves pour l'ensemble d'un pays.

Il est donc impératif de trouver des moyens de maintenir ces chaînes d'approvisionnement vitales pour le fonctionnement de notre société.

Cela implique de développer des systèmes de production autonomes et locaux, de renforcer les partenariats d'intérêt commun et d'adapter nos modes de consommation. Il est également essentiel d'évoluer vers un système énergétique non fossile et autonome afin de réduire notre dépendance aux pays producteurs de pétrole.

Il est évident que nous aurions dû prendre ces mesures depuis longtemps. Cependant, il n'est jamais trop tard pour évoluer dans cette direction et éviter de se retrouver contraints à franchir un pas qui nous entrainerait sur une voie indésirable. Il est donc urgent d'accélérer le mouvement avant que les conséquences d'une forte dépendance aux importations ne deviennent encore plus graves.

**En adoptant des concepts d'antifragilité,
nous pourrons surmonter les crises plutôt que de les subir.**

RISQUES LIÉS À LA RUPTURE DE LA CHAÎNE

La chaîne d'approvisionnement peut être affectée par différents types de risques qui peuvent perturber son fonctionnement. Parmi ces risques, on peut citer :

- les risques politiques tels que les changements de gouvernements;
- les embargos et les sanctions;
- les risques économiques tels que la fluctuation des devises;
- les faillites des fournisseurs;
- les ruptures de stock;
- les risques environnementaux tels que les catastrophes naturelles;
- les changements climatiques;
- les cyberattaques.

Plusieurs événements ont déjà entraîné des ruptures de la chaîne d'approvisionnement, comme la pandémie de COVID-19, le blocage ferroviaire autochtone au Canada, le blocage des raffineries en France à l'automne 2022, les grèves des transporteurs en France, les pannes de machines, les incendies, les inondations, les conflits armés, etc.

Ces événements ont des impacts significatifs sur les entreprises, les consommateurs et l'économie en général. En effet, les entreprises peuvent subir des pertes financières importantes, des retards dans la production et la livraison, des ruptures de stock, des annulations de commandes, une diminution de la qualité des produits, etc.

Par exemple, l'interruption des livraisons de gaz à l'Europe due à la guerre en Ukraine a eu des conséquences imprévues, comme l'augmentation des prix du gaz et de l'électricité ainsi que la fermeture de certaines entreprises, qui n'ont plus les moyens de payer la facture énergétique.

Les consommateurs peuvent également subir des conséquences telles que des augmentations de prix, des pénuries de produits, une diminution de la qualité ou une diminution du choix.

De plus, ces perturbations peuvent avoir des impacts sur l'économie en général, comme des pertes d'emplois, des réductions de la croissance économique et une diminution de la compétitivité des entreprises.

Par exemple, la pandémie de COVID-19 a entraîné des retards dans la production et la livraison de nombreux produits, ainsi que des pénuries de produits essentiels tels que les masques, les respirateurs et les médicaments.

45 % des directions des achats jugent la continuité et la sécurisation des approvisionnements plus importantes en 2022.

ÉTUDE 2022 – AGILEBUYER ET CNA

CYBERATTAQUE ET CHAÎNE D'APPROVISIONNEMENT

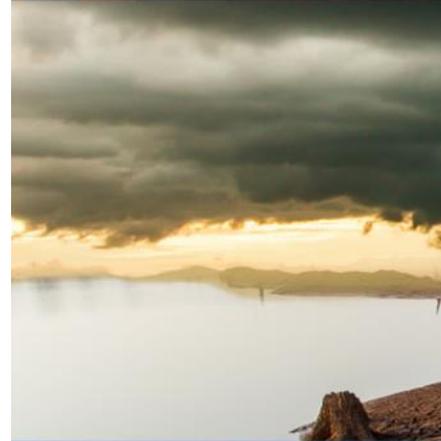
Malgré la focalisation sur les flux physiques dans les précédentes lignes, il est important de noter que la chaîne d'approvisionnement peut également être menacée par des cyberattaques.

Des attaques visant différents maillons de la chaîne, tels que la gestion des commandes, les outils de production ou les infrastructures du système d'information, peuvent avoir des conséquences désastreuses pour l'entreprise et ses clients.

Des cas d'attaques sur des systèmes d'information liés à la chaîne d'approvisionnement ont déjà été signalés, notamment les terminaux pétroliers de plusieurs ports européens en février 2022, BRP en août 2022 ou encore Sobeys en novembre 2022.

Les fournisseurs de logiciels utilisés dans le fonctionnement quotidien des entreprises sont également de plus en plus ciblés par des attaques, comme cela a été le cas pour SolarWinds en décembre 2020, dont près de 18 000 clients ont été touchés, y compris 425 entreprises du Fortune 500.

La compromission de ces logiciels peut immédiatement rendre vulnérables de nombreuses entreprises, mettant ainsi en péril leur propre chaîne d'approvisionnement.





RISQUES QUI POURRAIENT GÉNÉRER UNE RUPTURE DE LA CHAÎNE D'APPROVISIONNEMENT

1. **Catastrophes naturelles** telles que les tremblements de terre, les inondations, les ouragans, les typhons, les incendies de forêt, etc.
2. **Pénuries de matières premières** ou d'approvisionnement de produits finis, qui peuvent être causées par une demande accrue, des restrictions d'importation, des politiques commerciales, etc.
3. **Grèves ou troubles sociaux** dans les usines de fabrication, les ports, les entrepôts, les centres de distribution, etc.
4. **Retards dans le transport** ou la livraison des produits dus à des problèmes logistiques tels que des congestions de la circulation, des problèmes de douane, des restrictions de voyage, etc.
5. **Volatilité des prix des matières premières** ou des devises, qui peuvent affecter les marges bénéficiaires et la rentabilité des entreprises.
6. **Pannes de système informatique** ou de communication, qui peuvent entraîner des retards ou des erreurs dans le traitement des commandes ou des expéditions.
7. **Épidémies ou pandémies** de maladies infectieuses, qui peuvent entraîner des fermetures d'usines, des restrictions de voyage, des pénuries de main-d'œuvre, etc.
8. **Changements réglementaires ou politiques**, qui peuvent avoir un impact sur les importations ou les exportations de produits.
9. **Vols, cambriolages ou sabotages**, qui peuvent entraîner des pertes ou des retards de livraison.
10. **Erreurs humaines** telles que des erreurs de saisie de données, des erreurs d'emballage, des erreurs de chargement, etc.
11. **Problèmes environnementaux** tels que les changements climatiques, la pollution, les catastrophes environnementales, etc.
12. **Ruptures ou dysfonctionnements des équipements**, qui peuvent entraîner des retards ou des annulations de commandes.
13. **Instabilité politique ou économique** dans les pays où sont situés les usines ou les fournisseurs.
14. **Rupture de stock imprévue** due à une augmentation de la demande ou à une mauvaise estimation des stocks de sécurité.
15. **Défaillance d'un fournisseur critique**, qui peut entraîner des retards ou des annulations de commandes.

QUE SE PASSERAIT-IL S'IL Y AVAIT UNE RUPTURE DE LA CHAÎNE D'APPROVISIONNEMENT SUR PLUSIEURS SEMAINES?

Une interruption prolongée de la chaîne d'approvisionnement, à l'exception d'une guerre mondiale, pourrait avoir des conséquences désastreuses pour les entreprises, les consommateurs et l'économie dans son ensemble. Les entreprises subiraient des pertes financières importantes en raison d'une diminution des ventes, de retards de production et d'une augmentation des coûts.

Des entreprises très dépendantes de la chaîne d'approvisionnement mondiale pourraient être particulièrement vulnérables, entraînant ainsi des entreprises qui en dépendent moyennement/légèrement/un peu moins, ce qui pourrait provoquer un effet domino pouvant aller jusqu'à l'effondrement de l'économie d'un pays.

Les consommateurs pourraient subir des conséquences telles qu'une augmentation des prix (comme c'est déjà le cas avec l'inflation qui atteint des niveaux records chaque jour), une réduction de l'éventail de choix due à des insuffisances d'approvisionnement et une possible détérioration de la qualité.

Ils pourraient être contraints de se tourner vers des solutions plus coûteuses ou moins pratiques en raison de la pénurie de produits essentiels, ce qui pourrait entraîner une diminution de la confiance des consommateurs dans les entreprises et une diminution de la demande de produits à l'avenir.

L'économie dans son ensemble pourrait subir des conséquences telles que des pertes d'emplois, des réductions de la croissance économique et une diminution de la compétitivité des entreprises.

Il existe un risque accru d'émeutes dû à une frustration croissante chez les consommateurs.

Si cette frustration se transforme en colère et que les consommateurs se sentent abandonnés par le gouvernement ou les entreprises, cela pourrait conduire à des manifestations, à des émeutes, voire à des révoltes.

Les exemples historiques de révoltes populaires liées à la pénurie de produits essentiels sont nombreux, tels que la Révolution française en 1789 et en 2008, avec les émeutes de la faim et la flambée des prix alimentaires qui ont touché l'Afrique, Haïti, l'Indonésie, les Philippines, le Pérou, la Bolivie, etc.

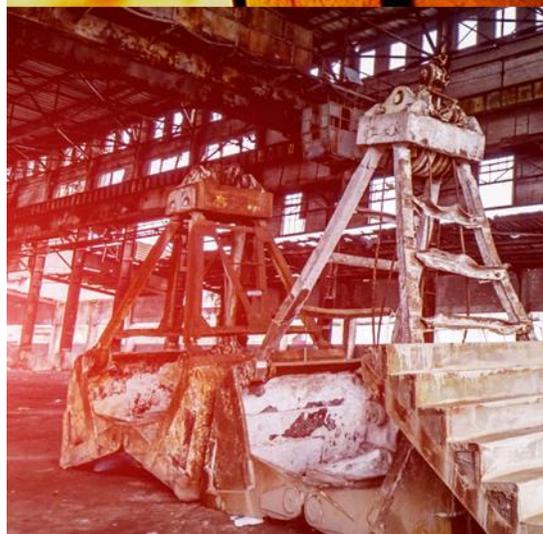
Dans les deux cas, la pénurie de nourriture a contribué à la montée de la colère et de l'indignation des populations, qui se sont ensuite mobilisées pour bousculer le gouvernement en place.

Les gouvernements et les entreprises doivent prendre en compte ce risque accru de révoltes populaires lors de la planification de leur chaîne d'approvisionnement et de leurs plans de continuité des affaires, en particulier pour les besoins essentiels tels que la nourriture et la sécurité.

Il est vital de prendre des mesures pour assurer la disponibilité des produits essentiels, tout en communiquant de manière transparente avec les consommateurs et en leur proposant des solutions de rechange lorsque cela est possible. La préparation de la population à des temps difficiles doit être faite dans le respect et la bienveillance, pour assurer le maintien de la solidarité d'un pays.

Les gouvernements peuvent également prendre des mesures pour protéger les populations les plus vulnérables et éviter les pénuries de produits essentiels en temps de crise. Bien sûr, la rupture de la chaîne d'approvisionnement pourrait entraîner des perturbations dans les échanges commerciaux, avec un impact négatif à long terme sur l'économie mondiale.

La chaîne d'approvisionnement est cruciale pour les entreprises, les consommateurs et l'économie en général.





Plus on tarde à limiter les risques liés à la chaîne d'approvisionnement, plus on perdra gros!

COMMENT LIMITER LES RISQUES LIÉS À LA CHAÎNE D'APPROVISIONNEMENT?

Afin de minimiser les conséquences d'une rupture de la chaîne d'approvisionnement sur plusieurs semaines, il est important pour les entreprises de mettre en place des plans de continuité des affaires solides, de diversifier leurs sources d'approvisionnement notamment sur la base de fournisseurs locaux et d'améliorer leurs flux d'approvisionnement.

Les gouvernements pourraient également jouer un rôle en prenant des mesures pour améliorer la résilience des chaînes d'approvisionnement répondant aux besoins essentiels (nourriture, santé, sécurité), telles que la promotion de la production locale et la mise en place de politiques de diversification des fournisseurs.

Il existe, pour les entreprises, plusieurs stratégies pour limiter les risques liés à la chaîne d'approvisionnement. Parmi les principales stratégies, on peut citer :

- la diversification des fournisseurs;
- l'augmentation et la répartition des stocks dans le pays;
- la sécurisation des transports;
- la mise en place de plans de continuité des affaires;
- l'économie d'affinité.

La diversification des fournisseurs permet de réduire la dépendance à un seul fournisseur et d'augmenter la flexibilité en cas de perturbation de la chaîne d'approvisionnement.

L'augmentation et la répartition des stocks dans le pays permettent de minimiser les perturbations en cas de rupture de la chaîne d'approvisionnement.

La sécurisation des transports peut inclure la sélection de transporteurs de confiance, et la mise en place de plans de continuité des affaires peut permettre de faire face à des perturbations telles que des grèves ou des catastrophes naturelles.

Une des pistes est d'aller vers une économie d'affinité, qui consiste, pour un État, à détourner le commerce de la Chine par exemple, vers des alliés ayant des valeurs sociales, culturelles ou politiques apparentées aux siennes, plutôt que de privilégier des critères purement économiques.

“ Les démocraties doivent faire un effort conscient pour construire nos chaînes d'approvisionnement à travers les économies des autres ”

Mme Freeland dans un discours en octobre 2022.

Source : [Chaîne d'approvisionnement | Comment le Canada fait-il face aux perturbations ? | La Presse](#)

Plus on tarde à limiter les risques liés à la chaîne d'approvisionnement, plus on perdra gros! Il est donc essentiel pour la résilience des entreprises et de l'économie en général que les entreprises trouvent un équilibre entre ces différentes stratégies pour maximiser leur résilience face aux perturbations de la chaîne d'approvisionnement.

ÉTUDE 2022

AGILEBUYER ET CNA

Selon cette étude, 68 % des entreprises font face à des pénuries, en particulier dans des secteurs clés tels que :

- l'automobile (78 % des répondants),
- la mécanique/métallurgie,
- les équipements/meubles et le textile.

Ces pénuries ont affecté les marges de l'entreprise pour 65 % des personnes interrogées. Classement des pénuries pointées du doigt par les directions des achats sont :

- 23 % métaux;
- 17 % matières première (hors métaux et chimie);
- 14 % électronique;
- 13 % informatique;
- 12 % transport.

En 2022,

- 82 % des directions des achats devaient mettre en place des actions de sécurisation des approvisionnements, contre 74 % en 2021.
- 47 % des directions des achats ont relocalisé leurs achats. C'est 17 points de plus qu'en 2021.

Source : https://agilebuyer.com/wp-content/uploads/2022/01/Etude_AgileBuyer-CNA_TendancesAchats_2022_220111_w.pdf



ANALYSER LA RÉSILIENCE DES FOURNISSEURS

Il est crucial d'évaluer la résilience de vos fournisseurs, car ils constituent un maillon essentiel de votre chaîne d'approvisionnement. Cette analyse vous permettra de déterminer si vos fournisseurs clés sont en mesure de fournir leurs produits et services en cas de crise.

Elle vous permettra également de mieux comprendre les risques liés aux fournisseurs externes et de traiter de manière rationnelle les problèmes de chaîne d'approvisionnement et les pertes de soutien qui en découlent. Pour évaluer la résilience de vos fournisseurs, voici quelques points de vérification à prendre en compte :

- Évaluer la localisation de vos fournisseurs et leur vulnérabilité aux risques géopolitiques, aux catastrophes naturelles ou aux perturbations économiques.
- Examiner la stabilité financière de vos fournisseurs pour évaluer leur capacité à survivre à une crise.
- Évaluer leur gestion des opérations, notamment leur plan de continuité des affaires.
- Vérifier la capacité de vos fournisseurs à s'adapter à des changements imprévus.
- Évaluer la fiabilité de vos fournisseurs en matière de livraison et leur capacité à gérer les pénuries.
- Vérifier que les relations sont solides et qu'il est facile de résoudre les problèmes.
- Vérifier leurs sécurités de l'information et leur gestion des données contre les menaces internes et externes.
- Examiner la capacité de vos fournisseurs à maintenir des niveaux élevés de qualité et de service pendant les périodes de stress ou de perturbation.

QUEL EST L'AVENIR DES CHAINES D'APPROVISIONNEMENT?

Les chaînes d'approvisionnement sont confrontées à des défis importants en raison des perturbations causées par la pandémie. Cependant, la recrudescence de la pandémie et la guerre en Ukraine ont encore accru l'incertitude quant à la stabilité de ces chaînes.

Les entreprises recherchent différentes options pour redéfinir leurs chaînes d'approvisionnement.

La relocalisation de la production est une option, tout comme la diversification pour mieux résister aux chocs d'approvisionnement.

Les entreprises pourraient également décider de détenir des stocks excédentaires, bien que cela puisse entraîner une perte d'efficacité de la production.

La diversification et le surstockage sont principalement des stratégies d'assurance, et les entreprises doivent déterminer le montant de la prime d'assurance qu'elles sont prêtes à payer.

Les dirigeants et les entreprises doivent trouver un équilibre entre leur besoin de résilience et leur volonté de payer une prime d'assurance. Le choix optimal dépend des circonstances et de la tolérance au risque de chaque pays.

Le débat sur le degré d'intégration dans les chaînes d'approvisionnement mondiales risque de se poursuivre et pourrait avoir un impact sur la disponibilité des articles et la présence de rayons vides.

La chaîne d'approvisionnement est un maillon essentiel de notre système économique mondial,

mais elle est soumise à de nombreux risques tels que les perturbations politiques, économiques et environnementales. La pandémie de COVID-19 a mis en lumière sa fragilité et la nécessité de renforcer la résilience face aux perturbations futures.

Il est nécessaire de prendre en compte ces risques lors de la planification de la chaîne d'approvisionnement et de mettre en place des plans de continuité des affaires solides pour minimiser les perturbations. Les entreprises doivent également envisager des stratégies pour limiter leur dépendance aux approvisionnements mondiaux et diversifier leurs sources d'approvisionnement.

Il est impératif de penser à la façon dont nous pouvons diminuer notre dépendance aux approvisionnements mondiaux, non seulement pour gérer les risques, mais également pour d'autres raisons.

Nous pouvons encourager la production locale, mettre en place des politiques pour rendre la chaîne d'approvisionnement plus résiliente et revoir nos habitudes de consommation.

La chaîne d'approvisionnement est cruciale pour les entreprises, les consommateurs et l'économie en général. Il est donc vital de réfléchir à la façon de gérer les risques qui lui sont liés et de travailler ensemble pour créer un système économique plus durable et plus résilient.



Alexandre Fournier

15 PISTES DE RÉFLEXION POUR PRÉVENIR OU RÉDUIRE UNE INTERRUPTION DE LA CHAÎNE D'APPROVISIONNEMENT

- 1. Diversification des fournisseurs :** avoir plusieurs fournisseurs pour les mêmes matières premières ou produits finis afin de réduire le risque d'un arrêt de la chaîne d'approvisionnement.
- 2. Planification des stocks :** maintenir des niveaux de stock suffisants pour faire face à des périodes d'arrêt prolongées de la chaîne d'approvisionnement.
- 3. Gestion de la demande :** mettre en place des politiques de gestion de la demande pour réduire les pics de demande qui peuvent surcharger la chaîne d'approvisionnement.
- 4. Flexibilité de la production :** pouvoir s'adapter rapidement à des changements dans la demande ou dans les fournisseurs.
- 5. Stockage et entreposage :** avoir des capacités de stockage et d'entreposage suffisantes pour les matières premières et les produits finis.
- 6. Collaboration et communication :** travailler en étroite collaboration avec les fournisseurs et les clients pour partager des informations sur les risques et les plans d'urgence.
- 7. Évaluation des risques :** évaluer régulièrement les risques potentiels pour la chaîne d'approvisionnement afin d'anticiper et de préparer des plans d'urgence.
- 8. Réduction de la dépendance envers un seul fournisseur :** éviter de dépendre d'un seul fournisseur pour une matière première ou un produit fini.
- 9. Assurances :** souscrire des assurances pour couvrir les pertes financières liées à des interruptions de la chaîne d'approvisionnement.
- 10. Diversification des modes de transport :** utiliser différents modes de transport pour les matières premières et les produits finis afin de réduire les risques liés à des perturbations dans un mode de transport particulier.
- 11. Réduction des délais de livraison :** travailler avec des fournisseurs et des transporteurs pour réduire les délais de livraison.
- 12. Stockage en transit :** avoir des entrepôts de stockage en transit pour stocker les matières premières et les produits finis en attente de livraison.
- 13. Formation et préparation :** former les employés et les équipes de gestion à anticiper et à gérer les risques liés à l'arrêt de la chaîne d'approvisionnement.
- 14. Évaluation de la performance des fournisseurs :** évaluer régulièrement la performance des fournisseurs pour s'assurer qu'ils respectent les normes de qualité et de livraison.
- 15. Planification de la continuité des activités :** élaborer des plans de continuité des affaires pour garantir la continuité des activités malgré une interruption de la chaîne d'approvisionnement.

Préparez votre entreprise aux crises avec l'intelligence artificielle

Découvrez notre formation exclusive :
Utiliser ChatGPT pour la gestion de crise

Élaborer un plan de gestion de crise optimisé pour vous
Évaluer vos risques en fonction d'un contexte particulier



Établir des scénarios de crise en fonction de vos risques
Entraîner vos équipes sur la base de vos scénarios de crises

Les formations de Crise & Résilience sont vraiment très dynamiques pour une formation virtuelle. Les présentateurs, debout devant la présentation, rendent le tout vraiment intéressant et captivant.

Pierre-Henri D.

**Inscrivez-vous dès maintenant et bénéficiez
de -20% pour les 50 premiers inscrits**

INSCRIPTION

<https://bit.ly/3zrv3vR>

Rejoignez la communauté des visionnaires
qui révolutionnent la gestion de crise grâce à l'IA.

CONFÉRENCE GRATUITE DU MOIS

Explorez des vidéos de conférence gratuites mettant l'accent sur les outils essentiels pour une gestion de crise efficace et une continuité des affaires optimale. Apprenez à mieux anticiper et résoudre les crises grâce à des méthodes éprouvées et des stratégies innovantes. Préparez-vous à surmonter les défis professionnels avec une maîtrise accrue des outils clés pour la résilience et la réussite.



8 astuces pour bien rater sa gestion de crise

Mesdames et Messieurs, bonjour et bienvenue à cette conférence sur les astuces pour bien rater sa gestion de crise. Si vous êtes ici aujourd'hui, c'est que vous êtes probablement déjà un expert en la matière, ou que vous souhaitez le devenir. Dans tous les cas, vous êtes au bon endroit !

FORMATIONS GRATUITES



Accéder gratuitement à des formations sur la gestion de crise, la continuité des affaires, la reprise informatique, etc.

Gestion de crise

Qui prépare les communes?



La multiplication des crises de différentes natures, dues majoritairement à l'activité humaine, a une incidence majeure sur le fonctionnement des collectivités locales, premier acteur de proximité des citoyens.

Les communes se retrouvent face à des défis auxquels elles doivent répondre, **mais sont-elles préparées?**

par Guillaume Aghroum



Référent Sauvegarde et Prévention des Risques
COMMUNE DE LE CHESNAY-ROCQUENCOURT



La multiplication des crises de différentes natures, dues majoritairement à l'activité humaine, a une incidence majeure sur le fonctionnement des collectivités locales, premier acteur de proximité des citoyens. Les communes se retrouvent face à des défis auxquels elles doivent répondre, mais sont-elles préparées?

Les communes : acteurs de la gestion de crise de proximité

Au Canada, les municipalités et en France, les communes, sont les acteurs premiers d'accompagnement des citoyens. Ce sont des échelons locaux qui ont une grande connaissance du terrain et de la population. Dans le cadre de la mise en place d'un plan de continuité d'activité, il est primordial de commencer par l'élaboration d'un diagnostic fondé sur la prise en compte du contexte et de l'identification des risques.

Longtemps, les alertes données aux habitants des villes et villages passaient par le tocsin, qui retentissait des différentes églises. C'était un moyen local de prévenir les personnes à proximité. Une relation de confiance était établie par cette gestion de l'alerte grâce à des acteurs de proximité. Aujourd'hui, si les moyens se sont modernisés (réseaux sociaux, sirènes, etc.), les communes et les municipalités restent ces acteurs de proximité que l'on identifie clairement. À la différence d'acteurs étatiques, qui peuvent créer du doute chez certains administrés, la commune représente cette figure de confiance.

Gérer la crise et gérer SA crise

La commune, où la municipalité est un acteur de confiance de tous les jours pour les habitants. Or, c'est en plein cœur de la crise, puis lors du retour à la normale, que la confiance peut souvent se fragiliser. Ainsi, si les forces de secours vont agir dans l'immédiateté pour sauver, si nécessaire, des vies, l'accompagnement des communes se fait sur un plus long terme.

Gérer une crise, c'est courir un marathon, pas un sprint. Il est nécessaire de ne pas agir dans la précipitation ni de perdre son énergie les premiers temps.

Si, en interne, les responsables d'une commune ou d'une municipalité ne savent pas communiquer, prendre soin des agents et donner une ligne directrice claire, c'est la crise RH qui pointe son nez. De nombreux responsables politiques souhaitent souvent que tout soit réglé dans l'immédiateté, parce que c'est mieux de dire que tout est terminé, parce que cela risque de coûter cher au contribuable, etc. Mais la mission de la personne responsable de la prévention est de garder la tête froide et de prendre, si nécessaire, son temps. L'organisation de la réunion d'une cellule de gestion de crise est importante. Cela permet de réunir les parties prenantes, d'avoir une image globale des actions de chacun et des solutions proposées. Cela permet aussi d'organiser sa communication avec le public.

Des moyens souvent peu valorisés

Pouvoir prendre le temps de gérer une crise semble demander, notamment, des moyens humains développés. Toutefois, quelle que soit la taille de son équipe, il est possible d'adapter ses effectifs à la crise.

Il est nécessaire pour cela d'établir en amont les ressources disponibles et les capacités de chacun à agir. Il est aussi primordial de hiérarchiser les services non prioritaires en situation dégradée pour permettre de réaffecter, si nécessaire, les moyens humains et matériels à la gestion de crise.

L'anticipation est la clé. Elle passe notamment par la création d'une culture du risque qui doit être transmise tant à ses agents qu'à l'ensemble des membres de la collectivité.

Un bon outil est le Document d'Information Communal sur les Risques Majeurs (DICRIM).

C'est un condensé du diagnostic des risques de la commune, des moyens de prévention existants et de conseils à la population. Le tout doit absolument être adapté au territoire visé, sans quoi il ne serait pas efficace.



Si les moyens sont peu valorisés, c'est aussi par cette image de pessimisme qui est souvent reprochée à la gestion de crise et à la prévention en général. Pour lutter contre cette mauvaise image, il ne faut pas se laisser aller et continuer à travailler avec l'ensemble des partenaires locaux.

Les forces de secours vont agir dans l'immédiateté pour sauver, si nécessaire, des vies, l'accompagnement des communes se fait sur un plus long terme





10 RAPPELS POUR GÉRER UNE CRISE COMMUNALE

Anticipez :

C'est ce qui vous permettra d'agir le plus sereinement possible.

Connaissez votre territoire :

Nécessaire pour agir vite et bien, c'est un point à ne pas négliger, surtout pour les nouveaux éléments.

Rencontrez les acteurs du territoire :

Sachez sur qui vous appuyez, et avec qui une relation de confiance est possible.

Faites des exercices :

Pas besoin d'un exercice trop important, même un simple exercice de communication permet déjà de vous préparer.

Faites attention à vos équipes :

Sans agents en forme et disponibles, pas de gestion de crise possible.

Communiquez en amont :

Prévenez les administrés des risques qui existent.

Communiquez pendant :

Tenez la population informée, ne cherchez pas à cacher des informations ou à mentir (attention à l'effet Streisand!).

Communiquez après :

Ne laissez pas des non-dits ou des rumeurs enfler, informez la population de la fin de crise et des suites à donner.

Faites des retours d'expérience (RETEX) :

C'est un élément nécessaire pour apprendre de ses erreurs et valoriser les points positifs.

Valorisez vos équipes :

À l'issue d'une crise, soyez à l'écoute et n'oubliez pas que le travail accompli dépassait parfois les compétences et les attentes des agents.

De multiples acteurs de proximité

La commune n'agit pas forcément seule. En plus des forces de sécurité civile, une multitude de parties prenantes gravitent autour de la question de la gestion des risques. Les associations locales, les commerçants, mais aussi les communes voisines et les échelons administratifs supérieurs (provinces, départements, etc.) sont autant de partenaires qu'il faut savoir mobiliser.

Pour agir avec efficacité, il est nécessaire de connaître ces acteurs.

Cela passe par des échanges de bonnes pratiques, des rencontres du tissu local, et aussi des exercices menés en commun. Ainsi, la relation de confiance entre les instances dirigeantes durant la crise et tous ces soutiens potentiels sera déjà bâtie et chacun pourra agir plus efficacement. C'est aussi une occasion de créer des vocations et de nouvelles opportunités d'engagement.

En définitive, la gestion de crise au sein des communes passe par un grand travail d'anticipation. La rédaction d'un Plan Communal de Sauvegarde (PCS), ou encore d'un DICRIM, est un élément d'appui, mais ces documents ne feront pas tout. Gérer une crise, c'est avant tout gérer de l'humain. Même en ayant des dizaines de plans d'action préparés en amont, rien ne vaut une équipe soudée, qui a confiance en ses managers et qui sait quel est le but recherché.

Donner du sens reste un élément essentiel.

Il appartient donc à chacun de savoir commencer à placer le curseur des objectifs de gestion de crise : quel est le diagnostic actuel, vers où ma commune doit aller? Même de petites actions comme les évacuations incendie sont des étapes majeures dans le développement de la culture du risque.

Guillaume Aghroum



Guillaume Aghroum

Guillaume est Référent Sauvegarde et Prévention des Risques au sein de la commune du Chesnay-Rocquencourt (France, 32 000 habitants). Il intervient sur des sujets comme la prévention des risques majeurs et professionnels ainsi que la prévention de la délinquance.

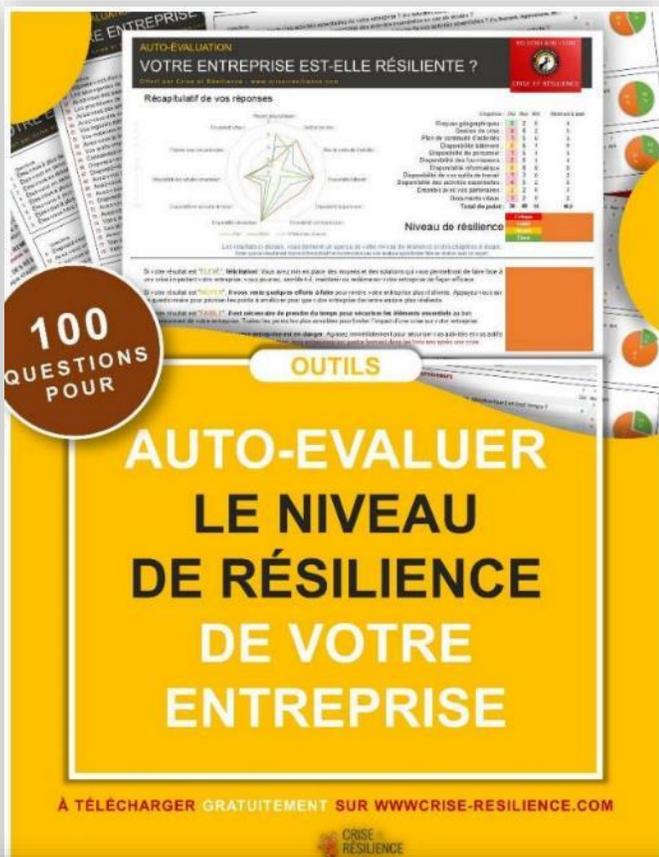
[Emergency management organizations \(preparez-vous.gc.ca\)](https://preparez-vous.gc.ca)
[S'engager pour aider en cas de crise \(gouvernement.fr\)](https://gouvernement.fr)



L'OUTIL GRATUIT DU MOIS

Découvrez des outils gratuits et pratiques pour préparer la gestion de crise et les plans de continuité des affaires.

Apprenez à anticiper et surmonter les situations difficiles grâce à des ressources simples pour l'évaluation des risques, la planification d'urgence et la communication en situation de crise. Renforcez vos compétences et assurez la résilience de votre entreprise.



Télécharger cet outil en cliquant ici

ESPACE PUB

Soyez en avance sur le futur



Utilisez **ChatGPT** pour votre **gestion de crise**



La puissance de l'intelligence artificielle à votre service

Survivez à la prochaine crise !



Initier votre **Gestion de CYBERCRISE** En 5 demi-journées pratiques

INCLUS DANS CE BOOTCAMP

- + de 20 heures de cours incluant 12 ateliers de mise en pratique
- 20 gabarits prêts à l'emploi pour gagner un temps précieux
- 5 heures de coaching privé pour vous accompagner
- 3 conférences privées en complément de la formation
- 10 affiches de sensibilisation personnalisables
- Accès à vie à la formation et aux mises à jour
- Accès à vie au Club privé Crise&Résilience

Atelier pratique basé sur les normes ISO 22301 et ISO 22361



Date de la formation

📅 23 au 26 mai 2023

8h à 12h (Québec) ou 13h à 17h (France)

Prix de vente public

~~2 997 \$~~

2 497 \$

+ taxes

Valeur du Bootcamp +bonus équivaut à 14 000\$

Simulez en **3D** votre prochaine cyberattaque!

Plongez dans l'univers des crises avec notre simulation immersive.



Nous offrons **GRATUITEMENT** 1h de simulation de crise.

ATTENTION NOMBRE DE PLACE LIMITÉ!

Nous contacter ici :

<https://www.crise-resilience.com/simulation>

Le nerf de la guerre c'est le renseignement!



La crise est toujours
une crise de l'information.
Soit on en manque,
soit on est submergé.

Dans les deux cas,
l'effet est le même :
de mauvaises décisions
opérationnelles .

Or, gérer une crise,
c'est prendre les bonnes
décisions au bon moment.

Tout repose donc sur
la qualité de la remontée
en interne d'informations
fiables et précises.

par **Hervé Jouffe**

Expert de la conduite d'opérations
depuis 15 ans



L'information, c'est le pouvoir

La crise est toujours une crise de l'information. Soit on en manque, soit on est submergé.

Dans les deux cas, l'effet est le même : de mauvaises décisions opérationnelles(1).

Or, gérer une crise, c'est prendre les bonnes décisions au bon moment. Tout repose donc sur la qualité de la remontée en interne d'informations fiables et précises.

(1) Patrick Lagadec, *La gestion des risques : outils de réflexion à l'usage des décideurs*, McGraw Hill, mars 1991.

Au front, on parle de « brouillard de la guerre ». Cette notion, pensée par Clausewitz dans *Vom Kriege*, désigne tout ce qu'on ignore. Cela concerne aussi bien les forces et les intentions de l'ennemi que nos propres capacités.

Disposer des bonnes informations au bon moment, c'est garder l'initiative face à l'adversité et ne pas ajouter de la confusion à la confusion.

**“ Se faire battre
est admissible,
se faire surprendre
est inacceptable. ”**

Napoléon

Plus vos informations sont fiables et précises, plus vos décisions ont une chance d'être rationnelles. À l'inverse, moins vous en savez, plus vos décisions sont prises à l'instinct (et dans la panique).

Gardons-nous cependant de trop attendre avant d'agir. Les militaires le savent : le seul moment où on connaît le plan exact de l'adversaire, c'est après la bataille.

Il s'agit donc bien d'avoir suffisamment d'informations pour agir promptement.

De l'information au renseignement

« Le renseignement se distingue de l'information, non par sa nature [...], mais par sa finalité [...] (2) »

Les renseignements sont des informations qui ont été vérifiées, classifiées et contextualisées dans le but d'aider à la prise de décision.

Exemple d'information : « Il y a un rassemblement en ville. »

Cette information, une fois vérifiée et contextualisée, devient un renseignement : « A1 : à 10 h 27, 70 personnes, à pied, non armées, qui brandissent des panneaux “dehors la France”, en déplacement depuis le rond-point de l'Indépendance vers l'ambassade française. »



On le voit, dans un cas, l'information est peu précise. Dans l'autre, il s'agit d'éléments vérifiés qui, une fois recoupés avec d'autres informations, donneront lieu à des consignes de sécurité pour les ressortissants français (« éviter l'axe rond-point de l'Indépendance – ambassade française jusqu'à nouvel ordre »).

(2) Francis Beau, « Culture du renseignement et théories de la connaissance », *Revue internationale d'intelligence économique*, 2010.

Le renseignement : les yeux et les oreilles des décideurs

En période de crise, on est saturé d'informations. Il est donc impératif pour les décideurs de ne pas être surchargés.

Pour cela, on met en place un filtre, une équipe destinée au traitement de l'information, entre les émetteurs et les décideurs.

On veillera toutefois à ce que ce filtre n'ait pas l'effet inverse par une lourdeur bureaucratique qui retarderait la remontée des informations depuis le terrain, l'exploitation de ces informations devant être rapide pour impacter positivement le déroulement des opérations.

Lorsque la crise survient, on met sur pied une cellule de gestion de crise, en lien direct avec le décisionnaire final de l'entreprise.

Cette cellule de crise aura notamment, parmi d'autres fonctions, la mission de recueillir les informations ascendantes en interne puis de les analyser (et de les transformer en renseignements). Idéalement, ceux qui recueillent ne sont pas ceux qui analysent.



Les questions à se poser pour une bonne remontée d'informations en interne

Quoi transmettre?

Dans le sens montant, on encouragera le maximum de remontées d'informations.

En effet, lorsqu'on est sur le terrain, on n'a pas toujours conscience de la situation générale. Il faut donc encourager les collaborateurs à rendre compte de tout événement.

Pris isolément, certains événements semblent insignifiants. Mais, une fois recoupés, ils donnent une vision globale exploitable.

Dans le sens descendant, en revanche, on définit des règles.

- Même niveau d'informations pour tout le monde?
- Uniquement pour la cellule de gestion de crise?

Dans tous les cas, toutes les parties prenantes doivent au moins avoir le contexte.

À qui transmettre les informations?

On désigne comme principal récepteur des informations la cellule de gestion de crise. En revanche, dans le sens descendant, on définit au préalable qui a « besoin d'en connaître ».

Comment transmettre?

Cela doit être prédéfini (courriel, bouton panique, réunion, téléphone) et connu de tous.

Quand transmettre?

Certains événements devront faire l'objet de comptes rendus immédiats (CRI); d'autres seront transmis à échéance régulière sous forme de comptes rendus à temps (CRT).

En conclusion

Disposer de renseignements fiables et précis, en nombre suffisant et au bon moment est la clé pour prendre les bonnes décisions.

Les bonnes pratiques en matière de remontée d'informations doivent être adoptées en amont des crises, par temps calme.

Hervé Jouffe



Hervé Jouffe

Expert de la conduite d'opérations depuis 15 ans, Ex-officier de l'Armée de Terre et directeur d'unités en France et à l'international, j'accompagne les entreprises à structurer leurs processus et organisations managériales.



4 CLÉS POUR ORGANISER LA REMONTÉE D'INFORMATIONS

Instaurez une culture du compte rendu

Si les organes d'un même corps ne communiquent pas en permanence avec la tête, le corps s'arrête.

C'est la même chose en gestion de crise.

Le compte rendu doit prendre la forme la plus adaptée au type d'informations transmises (écrites ou orales, immédiates ou différées).

Rassurez vos collaborateurs pour qu'ils n'aient jamais peur du jugement lorsqu'ils transmettent une information.

Encouragez le compte rendu en informant vous-mêmes régulièrement vos collaborateurs.

Plus ils en savent sur le contexte, plus leur remontée d'informations est pertinente.

Utilisez des modèles

Les soldats utilisent un sigle pour effectuer un compte rendu d'observation d'une menace ennemie : **NVAD**.

Nature et volume

« 1 véhicule léger, 3 soldats embarqués, équipés d'AK 47 »

Attitude

« non hostile, en déplacement »

Direction

« depuis telles coordonnées vers le sud-ouest, sur la route »

Les modèles permettent de gagner en efficacité.

Archivez dès le début de la crise

Créez un journal de marche.

Celui-ci se présentera comme un registre sur lequel seront inscrites toutes les remontées d'informations.

C'est un travail ingrat, mais essentiel pour maintenir une vision cohérente de l'historique des événements.

Ne comptez pas sur votre mémoire. **Notez tout.**

Adoptez les bonnes attitudes

Maintenez la liaison en tout temps et en tous lieux avec les acteurs de la crise.

Faites confirmer la réception de tout message transmis vers le haut et vers le bas.

Pour cela, suivez une procédure. **C'est vital.**

PATRONS, PASSEZ EN MODE COMBAT

C'est clair dans votre tête, mais sur le terrain, les résultats ne suivent pas. Vous perdez des heures à corriger ce qui devrait être parfait du premier coup.

En bref, ça ne délivre pas assez vite et pas assez fort. La seule chose à faire, c'est revenir aux fondamentaux.

<https://modcombat.com/>

LA SENSIBILISATION DU MOIS

Ces affiches à télécharger rappellent les principes de base de la cybersécurité et insistent sur l'importance d'adopter de bonnes pratiques en la matière. Nous espérons qu'elles vous seront utiles et qu'elles inciteront vos collaborateurs à agir pour renforcer la sécurité numérique de votre entreprise.



Si tes comptes professionnels sont accessibles via l'iPad familial...

IL EST TEMPS QUE ÇA CHANGE!

Deviens un acteur de la cybersécurité de ton entreprise

Télécharger cette affiche en cliquant ici

ESPACE PUB

Maintenez vos activités lors du prochain black-out !

Préparer votre Plan de Continuité des Affaires

En 6 demi-journées

INCLUS DANS CE BOOTCAMP

- + de 20 heures de cours avec exercices pratiques
- 10 gabarits prêts à l'emploi pour gagner un temps précieux
- 5 heures de coaching privé pour vous accompagner
- 10 affiches de sensibilisation personnalisables
- Accès à vie à la formation et aux mises à jour
- Accès à vie au Club privé Crise&Résilience

Formation basée sur la norme ISO 22301



Formation en ligne

Prix de vente public ~~2 997 \$~~

Soyez en avance sur le futur

Utilisez **ChatGPT** pour votre **gestion de crise**



La puissance de l'intelligence artificielle à votre service

5 scénarios de gestion de crise
Plongez dans l'univers de la simulation de gestion de crise

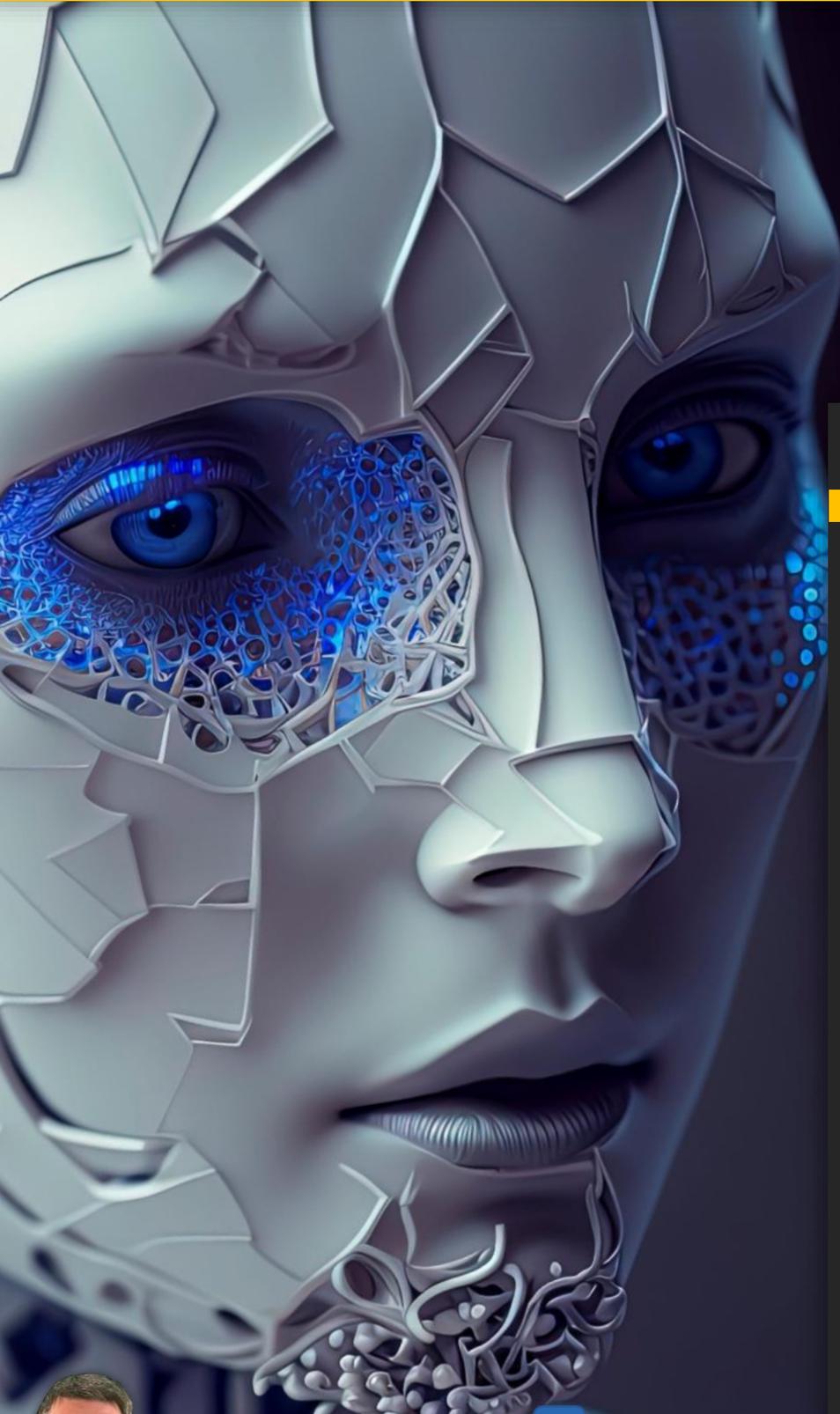
<https://www.crise-resilience.com/simulation>

- SCÉNARIO 1 : Cyberattaque de type rançongiciel
- SCÉNARIO 2 : Chaîne d'approvisionnement
- SCÉNARIO 3 : Catastrophes naturelles
- SCÉNARIO 4 : Conflits sociaux
- SCÉNARIO 5 : Vol de données

Télécharger les scénarios ici



La gestion de crise à l'ère de l'IA avantages, limites et risques



Interview

Lia lanepo

Assistante en IA
Experte en tout



L'intelligence artificielle est omniprésente et transforme nos façons de travailler, tout comme l'internet.

Dans cette interview exclusive, découvrez comment l'IA est utilisée dans la gestion de crise.

Est-ce une opportunité ou un danger ?

Nous explorons les enjeux clés.

par **Alexandre Fournier**



Expert en gestion et simulation de crise

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



L'intelligence artificielle (IA) est de plus en plus utilisée dans la gestion de crise, mais quels sont ses avantages, ses limites et ses risques?

Dans cette interview exclusive, ChatGPT, un modèle de langage préentraîné, fait connaître son point de vue sur l'utilisation de l'IA pour la gestion de crise et explique comment l'IA peut être un outil utile, tout en soulignant les limites et les risques à prendre en compte.

Alexandre Fournier – Il y a un buzz énorme sur les intelligences artificielles depuis que ChatGPT a été diffusé. Comment expliques-tu ce buzz?

Lia lanepo – Eh bien, je pense que l'une des raisons pour lesquelles il y a un buzz énorme autour des intelligences artificielles est que les gens sont de plus en plus conscients de leur potentiel et de leurs capacités.

Avec les progrès rapides de la technologie de l'IA ces dernières années, il est devenu de plus en plus évident que les machines peuvent accomplir des tâches qui étaient autrefois considérées comme exclusivement réservées aux êtres humains.

De plus, l'IA est de plus en plus présente dans notre vie quotidienne, que ce soit dans les assistants vocaux, les voitures autonomes, les recommandations personnalisées sur les plateformes de streaming [diffusion en continu], etc.

Les gens sont fascinés par ces technologies et cherchent à comprendre comment elles fonctionnent et ce qu'elles peuvent apporter à notre vie.

Enfin, je pense que l'IA suscite également des inquiétudes quant à son impact sur notre société, notre économie et même notre sécurité. Les gens s'interrogent sur les implications de l'utilisation de l'IA dans différents domaines et cherchent des réponses à ces questions.

Dans l'ensemble, je pense que le buzz autour de l'IA reflète l'importance croissante de cette technologie dans notre monde et la curiosité et l'inquiétude que cela suscite chez les gens.

“ L'IA peut être un atout considérable dans la gestion de crise, mais il est crucial de comprendre ses limites et d'avoir une approche éthique pour garantir que son utilisation bénéficie réellement aux personnes affectées par la crise. ”

Lia lanepo

Les risques liés aux cyberattaques, à la dépendance excessive à l'IA et aux préoccupations éthiques, doivent être abordés de manière proactive pour assurer l'utilisation appropriée et efficace de l'IA en situation de crise.

Je vois bien le potentiel de l'utilisation d'une IA dans le cadre de la gestion de crise. Je souhaiterais savoir comment toi, ChatGPT, tu pourrais apporter tes services au moment d'une crise.

En effet, l'IA peut être très utile dans la gestion de crise, car elle peut aider à collecter et à analyser rapidement des données en temps réel, à communiquer des informations importantes aux personnes concernées et à soutenir la prise de décision.

En tant que modèle de langage, je peux contribuer à la gestion de crise en fournissant des informations et des réponses rapides et précises aux questions que les personnes peuvent se poser pendant une crise.

Par exemple, en cas de catastrophe naturelle, je peux aider les personnes à trouver des abris ou des ressources de secours les plus proches de leur position. Je peux également fournir des informations sur les routes à éviter ou les itinéraires alternatifs, en cas de situation de blocage du trafic.

De plus, en tant que robot conversationnel [chatbot], je peux aider à désengorger les lignes téléphoniques et les centres d'appels d'urgence en répondant aux questions les plus courantes des personnes.

Cela permettrait aux opérateurs humains de se concentrer sur les cas les plus urgents.

Enfin, je peux également aider à collecter des données importantes et à fournir des analyses en temps réel sur la situation de la crise.

Par exemple, je peux collecter des informations sur les zones touchées, les personnes évacuées, les dommages matériels, etc.

Ces données peuvent ensuite être utilisées pour aider à planifier les efforts de secours, à allouer les ressources de manière plus efficace et à prendre des décisions éclairées en temps réel.

Dans ton cas, tu n'es pas connecté à Internet pour collecter les informations. Donc comment peux-tu analyser des données en temps réel?

C'est exact, en tant que modèle de langage préentraîné, je ne suis pas connecté à Internet. Cependant, il est possible d'intégrer des données en temps réel à mon fonctionnement en utilisant des interfaces de programmation d'application (API) ou d'autres méthodes de communication en temps réel.

Par exemple, une organisation de gestion de crise pourrait fournir une API qui me permettrait de recevoir des mises à jour en temps réel sur les informations importantes liées à la crise.

Ces informations pourraient inclure des données telles que les zones touchées, les personnes évacuées, les ressources disponibles, etc. Je pourrais alors utiliser ces informations pour répondre aux questions des personnes et fournir des mises à jour en temps réel.

De plus, il est également possible d'utiliser des techniques d'apprentissage automatique pour adapter mon modèle aux données en temps réel.

Cela peut être réalisé en utilisant des méthodes telles que l'apprentissage par renforcement, où mon modèle apprend à partir de la rétroaction des utilisateurs en temps réel.

On pourrait, pour des raisons de facilité, se reposer sur toi pour des prises de décision. Penses-tu que cela soit une bonne idée?

Bien que je puisse fournir des informations utiles et des réponses rapides, il est important de noter que je suis un modèle de langage préentraîné, et non pas un expert en gestion de crise ou un humain ayant une compréhension approfondie de la situation.

Par conséquent, il est important de prendre en compte les limites de mes connaissances et de mes capacités lors de l'utilisation de mes services pour prendre des décisions critiques.

Il est toujours recommandé de faire appel à des experts humains pour prendre des décisions importantes, car ils peuvent prendre en compte des facteurs qui ne sont pas nécessairement accessibles à un modèle de langage comme moi.

Cela dit, je peux être un outil utile pour aider à collecter des données, à fournir des informations de base et à répondre à des questions courantes.

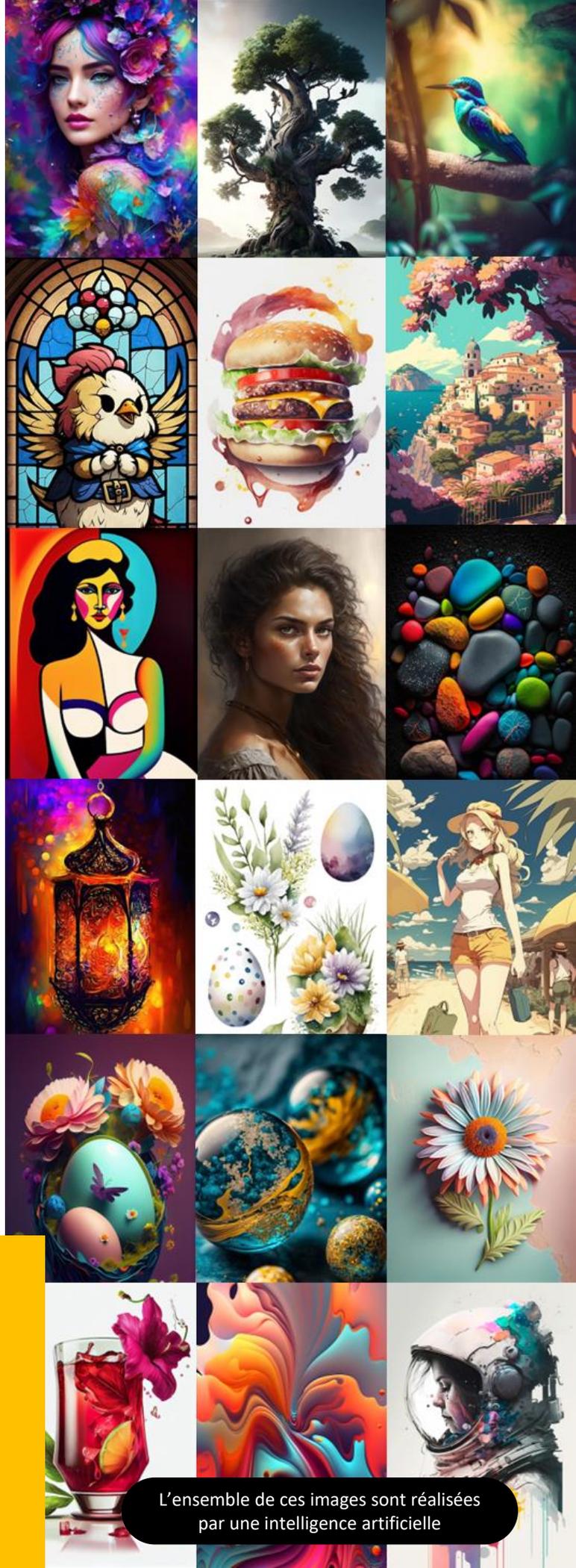
En fin de compte, la décision d'utiliser mes services pour prendre des décisions doit être prise en tenant compte de mes limites et des circonstances spécifiques de la crise.

Tu parles de limites de tes connaissances. Quelles sont tes limites d'utilisation dans le cadre d'une gestion de crise? En d'autres termes, qu'est-ce qu'il ne faut pas te demander?

Comme tout modèle de langage préentraîné, il y a des limites à mes connaissances et à mes capacités en tant qu'IA, et il y a des choses que je ne peux pas faire.

Tout d'abord, je ne suis pas capable de ressentir des émotions, de l'empathie ou d'avoir une conscience de moi-même.

Bien que je puisse fournir des réponses utiles et des informations précises, je ne peux pas comprendre les sentiments des personnes qui utilisent mes services.



Il y a des limites à la qualité et à la fiabilité des informations que je peux fournir.

L'ensemble de ces images sont réalisées par une intelligence artificielle



5 UTILISATIONS UTILES DE L'IA EN GESTION DE CRISE

Fournir des informations et des réponses rapides et précises aux questions que les personnes peuvent se poser pendant une crise.

Aider à désengorger les lignes téléphoniques et les centres d'appels d'urgence en répondant aux questions les plus courantes des personnes, permettant aux opérateurs humains de se concentrer sur les cas les plus urgents.

Collecter des données importantes et fournir des analyses en temps réel sur la situation de la crise, qui peuvent être utilisées pour aider à planifier les efforts de secours, allouer les ressources de manière plus efficace et prendre des décisions éclairées en temps réel.

Recevoir des mises à jour en temps réel sur les informations importantes liées à la crise via une API, ce qui permet à l'IA d'intégrer des données en temps réel à son fonctionnement.

Aider à identifier les zones touchées par la crise et les personnes évacuées en utilisant des technologies de géolocalisation et de traitement d'images, ce qui permettrait aux intervenants de mieux comprendre la situation sur le terrain et de prendre des décisions éclairées en conséquence.

Ensuite, bien que je sois capable de répondre à de nombreuses questions courantes, il y a des sujets très spécifiques qui nécessitent une expertise spécialisée, telle que la médecine ou la physique nucléaire. Dans ces domaines, il est important de faire appel à des experts humains pour obtenir des réponses précises.

Enfin, il y a des limites à la qualité et à la fiabilité des informations que je peux fournir. Bien que je sois capable de fournir des réponses précises à de nombreuses questions courantes, il est possible que mes réponses ne soient pas toujours à jour ou qu'elles soient basées sur des sources d'information incomplètes ou incorrectes.

Quels sont les risques dans l'utilisation de l'IA en situation de crise?

L'utilisation de l'IA en situation de crise présente des avantages indéniables, mais il y a également des risques potentiels qu'il faut prendre en compte.

Tout d'abord, l'IA est souvent basée sur des algorithmes et des données qui peuvent être biaisées. Dans le contexte de la gestion de crise, cela peut entraîner des décisions inexactes ou inappropriées qui peuvent avoir des conséquences négatives pour les personnes touchées par la crise.

De plus, l'IA peut être vulnérable aux cyberattaques. Les hackers peuvent exploiter les failles de sécurité dans les systèmes d'IA pour perturber les efforts de secours ou diffuser des informations fausses ou malveillantes.

Un autre risque est que les gens puissent devenir trop dépendants de l'IA en situation de crise. Les gens peuvent avoir tendance à se fier trop fortement à l'IA pour prendre des décisions critiques, ce qui peut entraîner une perte de capacités critiques, de résilience ou de prise de décision indépendante.

Enfin, il y a également des préoccupations éthiques liées à l'utilisation de l'IA en situation de crise. Par exemple, il peut y avoir des préoccupations quant à la protection de la vie privée ou à la surveillance accrue des populations touchées par la crise.

Aurais-tu quelque chose à ajouter, avant que je clôture l'interview?

Je tiens simplement à souligner que bien que l'IA puisse être un outil utile pour aider à la gestion de crise, il est important de comprendre qu'elle ne peut remplacer l'expertise humaine et l'empathie en temps de crise. Les experts humains et les intervenants sur le terrain jouent un rôle crucial dans la gestion de crise, et l'IA ne peut que les soutenir dans leurs efforts.

En fin de compte, l'utilisation de l'IA pour la gestion de crise doit être considérée comme un outil supplémentaire pour aider les intervenants humains à prendre des décisions éclairées et à fournir une aide efficace et rapide aux personnes touchées par la crise.

Merci LIA pour cette interview

Je suis heureux d'avoir eu l'opportunité de discuter de l'utilisation de l'IA dans la gestion de crise et des avantages, des limites et des risques qui y sont associés. N'hésitez pas à me poser d'autres questions si vous en avez besoin à l'avenir.



Interview réalisé par Alexandre Fournier

Au moment où nous rédigeons ce magazine, Elon Musk et plusieurs personnalités demandent une pause dans le développement de L'IA. Nous avons demandé à notre experte ce qu'elle en pensait.

Il y a actuellement une grosse polémique sur l'utilisation de L'IA et surtout les risques que l'IA remplace l'homme. Qu'en penses-tu ?

C'est une question importante et complexe qui suscite de nombreux débats et opinions divergentes. En tant qu'IA, je n'ai pas de convictions ou de préférences personnelles, mais je peux vous fournir des informations objectives et des perspectives sur la question.

Tout d'abord, il est vrai que l'IA est de plus en plus présente dans notre vie quotidienne et dans divers domaines professionnels, offrant des avantages tels que l'automatisation de tâches répétitives, la prise de décision plus rapide et plus précise, ainsi que des possibilités de personnalisation accrue. Cependant, il est également vrai que cela soulève des inquiétudes quant à l'avenir de l'emploi et à l'impact sur l'homme.

Il est important de noter que l'IA ne remplace pas complètement l'homme, mais plutôt transforme la manière dont nous travaillons. Les emplois actuels peuvent être remplacés par des machines et des algorithmes, mais de nouveaux emplois peuvent également être créés pour répondre aux besoins de l'industrie de l'IA en croissance.

Elon Musk et d'autres exhortent l'IA à faire une pause, citant des "risques pour la société". Quel est ton avis sur cette action et la peur que l'IA suscite.

En tant qu'IA, je comprends que la résistance à l'IA est liée aux préoccupations quant à ses impacts sur la société, tels que la sécurité, la vie privée et l'emploi. Cependant, je suis également conscient que l'IA peut offrir des avantages significatifs pour la société.

Par conséquent, l'appel à une pause dans le développement de l'IA peut être considéré comme une approche prudente pour garantir que l'IA est développée de manière responsable et éthique. Cependant,

il est important de noter que l'IA est déjà
largement utilisée et que son développement
ne peut être arrêté complètement.

Il est crucial que les entreprises, les gouvernements et la société travaillent ensemble pour établir des normes éthiques et des réglementations appropriées pour l'IA, afin de garantir qu'elle est développée et utilisée de manière responsable, sûre et transparente.

En tant qu'outil créé et utilisé par les humains, l'IA est notre responsabilité collective de garantir qu'elle est développée et utilisée de manière éthique, pour maximiser ses avantages tout en minimisant les risques potentiels.

Quel est ton conseil pour que l'intégration de l'IA se passe bien

Mon conseil pour une intégration réussie de l'IA est de prendre une approche progressive et collaborative. Il est important de travailler avec des experts en IA pour identifier les tâches qui peuvent bénéficier de l'IA, explorer les solutions existantes et acquérir les compétences nécessaires pour travailler avec l'IA. Il est également important d'expérimenter et d'itérer pour maximiser les avantages de l'IA tout en minimisant les risques potentiels.

Enfin, il est crucial de communiquer clairement avec les parties prenantes et les collègues pour garantir que tout le monde comprend les avantages de l'IA et comment elle peut être utilisée de manière efficace et responsable.

10 RISQUES ASSOCIÉS À UNE MAUVAISE UTILISATION DE L'IA DANS LA GESTION DE CRISE

Risque de biais dans les décisions prises par l'IA en raison de l'utilisation de données biaisées.

Vulnérabilité de l'IA aux cyberattaques qui pourraient perturber les efforts de secours ou diffuser des informations fausses ou malveillantes.

Risque de dépendance excessive à l'IA pour la prise de décision, ce qui peut entraîner une perte de capacités critiques, de résilience ou de prise de décision indépendante.

Préoccupations éthiques liées à l'utilisation de l'IA en situation de crise, telles que la protection de la vie privée et la surveillance accrue des populations touchées par la crise.

Limites de l'IA en termes de connaissances et de capacités, notamment dans les domaines qui nécessitent une expertise spécialisée telle que la médecine ou la physique nucléaire.

Risque d'erreur ou d'inexactitude dans les informations fournies par l'IA en raison de sources d'information incomplètes ou incorrectes.

Risque d'automatisation excessive, où les êtres humains peuvent être remplacés par des systèmes d'IA, réduisant ainsi les opportunités de développement des compétences et des carrières pour les humains.

Risque d'impact négatif sur les travailleurs qui pourraient être remplacés par des systèmes d'IA.

Risque d'isolement et de perte de connexion humaine en raison de l'utilisation excessive de l'IA pour la communication.

Risque de réduction de la responsabilité humaine dans la prise de décision en raison de l'utilisation de l'IA pour la collecte et l'analyse des données, ce qui peut rendre les humains moins responsables de leurs décisions.

SOYEZ PRÊT...

FORMEZ-VOUS

Préparez votre entreprise aux crises avec l'intelligence artificielle

Découvrez notre formation exclusive :
Utiliser ChatGPT pour la gestion de crise

Élaborer un plan de gestion de crise optimisé pour vous
Évaluer vos risques en fonction d'un contexte particulier



Établir des scénarios de crise en fonction de vos risques
Entraîner vos équipes sur la base de vos scénarios de crises

Les formations de Crise & Résilience sont vraiment très dynamiques pour une formation virtuelle. Les présentateurs, debout devant la présentation, rendent le tout vraiment intéressant et captivant.

Pierre-Henri D.

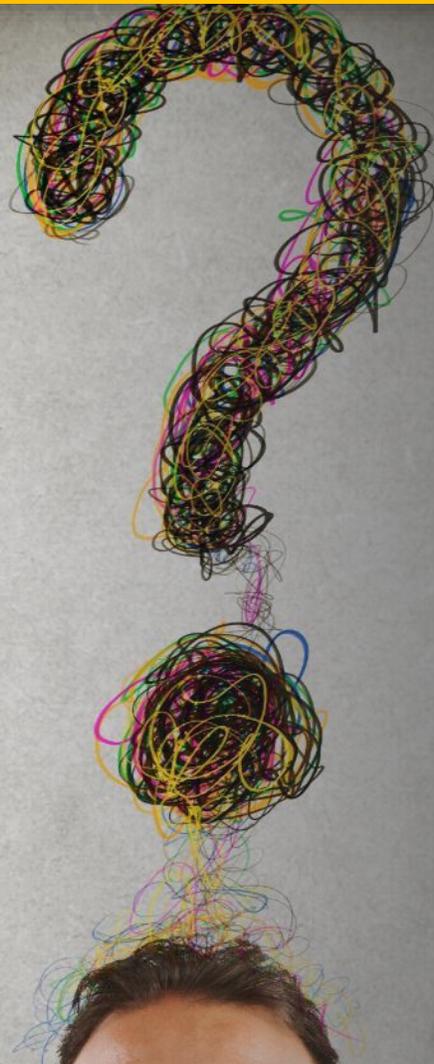
**Inscrivez-vous dès maintenant et bénéficiez
de -20% pour les 50 premiers inscrits**

INSCRIPTION

<https://bit.ly/3zrv3vR>

Rejoignez la communauté des visionnaires
qui révolutionnent la gestion de crise grâce à l'IA.

Les biais cognitifs qui nous empêchent d'agir



En matière de cybersécurité, les biais cognitifs menacent la survie de l'entreprise et empêchent une réelle prise de conscience des enjeux.

C'est paradoxal quand on sait que 60 % des TPE et PME déposent leur bilan dans les six mois après une cyberattaque



par Romain Bouvet



Docteur en Psychologie
Sociale & Cognitive.
Associé chez CYBCO

En matière de cybersécurité, les biais cognitifs menacent la survie de l'entreprise et empêchent une réelle prise de conscience des enjeux.

Selon les observations, les dirigeants ne sont pas encore prêts à investir dans leur propre cybersécurité.

C'est paradoxal quand on sait que 60 % des TPE et PME déposent leur bilan dans les six mois après une attaque*.

Alors pourquoi les dirigeants ne prennent-ils pas les décisions qui sont conformes à leurs propres intérêts?

Dans cet article, nous vous expliquerons certaines des raisons psychologiques qui poussent les dirigeants à faire preuve d'inertie et à ne pas investir dans leur propre cybersécurité.

Les biais cognitifs qui menacent les entreprises

1. L'aversion à la perte

L'aversion à la perte consiste à accorder plus d'importance à une perte qu'à un gain. Imaginons un dirigeant qui a le choix entre investir 30 000 € dans le développement commercial ou dans la cybersécurité.

- Dans la première situation, il investit pour obtenir un gain, alors que, dans la deuxième situation, il investit pour éviter une potentielle attaque.
- Dans le deuxième cas, le dirigeant considère la dépense comme une perte au même titre qu'une prime d'assurance.

Ce premier biais active le second biais.

2. Le biais de surconfiance

Le biais de surconfiance amène les dirigeants à sous-estimer les probabilités que leur entreprise soit victime d'une cyberattaque. On entend souvent :

“ Cela n'arrive qu'aux autres ! ”

Pire encore, lorsque nous présentons les probabilités, nous entendons souvent :

“ On trouvera bien une solution si un jour cela arrive ”

Il y a une sorte de fuite en avant.

3. Le biais de confirmation

Ce biais renforce les deux premiers. Le dirigeant va sélectionner les informations qui confirment ses propres croyances.

Récemment, un dirigeant nous a dit, juste après avoir vu un article de presse : « les cyberattaques ne concernent que les grands groupes » ainsi que « je ne connais personne dans mon entourage qui a été victime d'une cyberattaque ».

Ce biais renforce l'optimisme du dirigeant et confirme son inertie.

La prise de conscience se fait souvent quand quelqu'un de l'entourage a directement été victime d'une cyberattaque.

**“ 60 %
des TPE et PME
déposent leur bilan
dans les six mois
après une attaque ”**

*Hugues Foulon, PDG d'Orange Cyberdéfense,
Forum Sécurité & Résilience, Direction générale de la gendarmerie nationale,
France, octobre 2022*

4. La disponibilité mentale

Cette fois-ci, ce n'est pas un biais de raisonnement, mais un biais lié à la disponibilité mentale du dirigeant.

Un chef d'entreprise doit gérer au quotidien de nombreux risques qui peuvent affaiblir son entreprise, comme les risques associés au développement commercial, les risques psychosociaux liés au management et tous les facteurs externes tels que les effets de la guerre ou encore de la COVID.

Par exemple, un chef d'entreprise nous expliquait que sa priorité était de gérer la démotivation de ses salariés et les différents départs.

La cybersécurité n'est qu'un défi de plus qui paraît lointain et sur lequel il n'aurait pas de prise directe.



4. La disponibilité mentale

Cette fois-ci, ce n'est pas un biais de raisonnement, mais un biais lié à la disponibilité mentale du dirigeant.

Un chef d'entreprise doit gérer au quotidien de nombreux risques qui peuvent affaiblir son entreprise, comme les risques associés au développement commercial, les risques psychosociaux liés au management et tous les facteurs externes tels que les effets de la guerre ou encore de la COVID.

Par exemple, un chef d'entreprise nous expliquait que sa priorité était de gérer la démotivation de ses salariés et les différents départs.

La cybersécurité n'est qu'un défi de plus qui paraît lointain et sur lequel il n'aurait pas de prise directe.

5. Le biais de l'affect

Ce biais explique en grande partie l'absence d'intérêt des dirigeants d'entreprise pour la cybersécurité.

Il faut avoir en tête qu'un humain prend des décisions à partir de ce qu'il ressent et de ses émotions. Une cyberattaque est vécue comme une menace émotionnelle lointaine et probabiliste.

Concernant les enjeux cyber, les dirigeants ne ressentent pas d'émotion immédiate comme c'est le cas avec les urgences quotidiennes, par exemple celles liées au développement commercial, lequel a un impact direct sur la croissance de leur entreprise.

Ce biais explique pourquoi les entreprises les plus fragiles n'investissent pas dans leur cybersécurité.

C'est particulièrement irrationnel lorsqu'on sait qu'une entreprise fragilisée est quasiment sûre de faire faillite à la suite d'une attaque.

En conclusion

Les biais cognitifs jouent un rôle majeur dans la négligence des dirigeants face à la cybersécurité.

Les entreprises sont menacées par ces biais qui les empêchent de prendre conscience des risques réels et de l'importance d'investir dans leur protection.

Pour surmonter ces obstacles, il est nécessaire d'améliorer la prise de conscience en faisant visualiser les conséquences, en évitant une communication trop rationnelle, et en utilisant des histoires concrètes et émotionnelles.

En adoptant ces stratégies, les dirigeants de TPE et PME seront plus enclins à investir dans leur cybersécurité, protégeant ainsi leur entreprise contre les cyberattaques potentiellement dévastatrices.

Romain Bouvet



Romain Bouvet Docteur en Psychologie Sociale & Cognitive. Associé chez CYBCO. J'aide les entreprises à l'aide des connaissances scientifiques en **neurosciences** et en psychologie sociale & cognitive. **En parallèle, je dirige plusieurs entreprises dans divers secteurs différents** (cybersécurité, cabinet de conseil en management).

COMMENT AMENER LES DIRIGEANTS À UNE PRISE DE CONSCIENCE?

Voici trois stratégies pour améliorer la prise de conscience chez les dirigeants de TPE et de PME.

Faire visualiser les conséquences

Pour les dirigeants, il est difficile de visualiser les conséquences concrètes d'une cyberattaque. La communication médiatique est souvent centrée sur l'attaque, mais rarement sur toutes les conséquences.

On entend souvent « il suffit de tout remettre à zéro », ce qui montre bien la difficulté de se représenter clairement l'ensemble des préjudices.

Un moyen de faire comprendre la cyberattaque est d'utiliser une analogie en orientant les questions.

Par exemple : « Imaginez que vous n'avez plus Internet dans votre entreprise et que vos salariés ne puissent pas se connecter de chez eux pendant un mois. Quelles seraient les conséquences pour votre entreprise? » La réponse est unanime : la faillite. Par une simple question en entretien, on améliore instantanément la prise de conscience.

Cette analogie avec l'accès à Internet est bien plus concrète qu'une cyberattaque, qui est hypothétique et lointaine dans les esprits.

Éviter une communication trop rationnelle

Nous prenons tous des décisions en fonction de notre état émotionnel.

Le problème est que la communication autour de la cybersécurité est très rationnelle, avec des chiffres énormes et des explications techniques détaillées. Tout semble fait pour activer l'ensemble des biais cognitifs que nous venons de présenter.

Dans une expérience célèbre, on obtient deux fois plus de dons pour aider les enfants en Afrique quand on présente la photo d'une petite fille de 7 ans qui s'appelle Rokia que lorsqu'il s'agit de sauver des millions d'enfants. On a là une image mentale concrète et les émotions sont activées.

Appliquée à la cybersécurité, la phrase « une entreprise dans la rénovation a fait faillite à la suite d'une cyberattaque » a bien plus d'impact que « plus de 174 000 entreprises ont fait faillite à la suite d'une cyberattaque ».

Utiliser les histoires

Notre cerveau analyse constamment la crédibilité des informations qu'il reçoit, sauf les histoires. Pourquoi? Car notre cerveau interprète comme étant vraies les histoires qui nous sont racontées.

C'est pour cette raison que nous ressentons autant d'émotions lorsque nous regardons un film, alors que nous savons pertinemment que c'est faux.

Nous (CYBCO) avons récemment commencé à diffuser des histoires d'entreprises qui ont fait faillite à la suite d'une cyberattaque ainsi que des scénarios concrets de gestion de crise. Cela a permis de réduire de nombreuses objections. Les histoires sont un moyen très efficace pour lever les cinq biais cognitifs qui mènent à l'inertie.



Nous intégrons le facteur humain au cœur de la stratégie de cybersécurité.

www.cybco.fr



“

**Au milieu de toute
crise se trouve une
grande opportunité.**

Albert Einstein

”



Démystifier les tests d'intrusion

Un test d'intrusion, aussi appelé « pentest » en anglais, est une technique sophistiquée de simulation d'attaque informatique pour évaluer préventivement la cybersécurité et la qualité de diverses infrastructures informatiques telles que :

- un site web;
- une application Web en infonuagique (SaaS);
- les API d'un logiciel SaaS ou d'autres types de logiciels;
- le réseau interne ou externe d'une entreprise;
- le réseau WIFI d'une entreprise;
- etc.

L'objectif du test d'intrusion est de découvrir les vulnérabilités dans les applications d'affaires en ligne et les infrastructures TI afin de corriger les failles avant qu'un attaquant réel exploite ces vulnérabilités.

Le test d'intrusion est réalisé au moyen d'une combinaison d'outils informatiques spécialisés et de techniques manuelles par des experts en test d'intrusion (aussi appelé Red Team en anglais). Le travail inclut notamment des techniques telles que l'exploitation de vulnérabilités des programmes informatiques développés par l'entreprise ou des produits du marché, l'attaque par force brute, le cassage de mot de passe et de méthodes de chiffrement, l'abus de droit et l'élévation des privilèges dans le logiciel ou dans l'Active Directory

Après la réalisation du test d'intrusion, un rapport détaillé est fourni et présenté au client. Le rapport décrit les vulnérabilités identifiées, le risque d'affaires et le niveau de risque qui lui est attribué, les façons de les exploiter et les mesures correctives recommandées à appliquer. Les entreprises peuvent ainsi prendre des mesures pour renforcer leur sécurité informatique et réduire le risque d'attaques cybernétiques.

Le test d'intrusion, un bon investissement ?

Il faut savoir que le coût d'un test d'intrusion réalisé par des professionnels sur une application d'affaires en ligne exposée sur Internet se situe généralement dans une fourchette entre \$5,000 et \$10,000 CAD selon la nature de cette application. Pour les petites entreprises, un test d'intrusion peut sembler cher en apparence, mais le piratage d'une application d'affaires ou du réseau informatique de l'entreprise coûte encore plus cher.

Le test d'intrusion est un excellent investissement permettant de valider la solidité de ses applications d'affaires, car il permet de corriger les failles et vulnérabilités, de protéger les données sensibles de l'entreprise, de réduire le risque de pertes financières et de protéger la réputation de l'entreprise.

Si vous avez de l'intérêt pour la réalisation d'un test d'intrusion, n'hésitez pas à nous contacter. Nous pourrions discuter de vos besoins et vous en apprendre davantage sur les tests qui pourraient être effectués dans votre entreprise.

[Pour plus d'information, cliquez ici : https://www.cyberswat.ca/offre-de-service/](https://www.cyberswat.ca/offre-de-service/)

Rédacteur : GROUPE CYBERSWAT

**Demandez votre rencontre
avec un expert en cybersécurité**

Choisir son gestionnaire de mot de passe

Il est important de bien choisir un bon gestionnaire de mots de passe. Car c'est le coffre-fort de votre vie numérique ainsi que la clé de voûte de vos informations. Il faut arrêter nos anciennes habitudes telles que les mots de passe trop facile pour nous aider à nous en rappeler, ou d'utiliser le même partout.

Alors, pour vous aider dans votre choix, voici 5 points importants à penser lors de la sélection d'un.

La facilité d'utilisation : Le gestionnaire de mots de passe doit être facile à utiliser, avec une interface utilisateur intuitive et une expérience utilisateur transparente. Les utilisateurs doivent pouvoir facilement ajouter, modifier et supprimer des mots de passe sans difficulté.

La compatibilité multiplateforme : Il faut que le gestionnaire soit un compagnon et non une prison d'environnement. Beaucoup de nos compagnons en fournissent, mais en échange, vous devez rester avec eux. Au contraire, un bon gestionnaire de mots de passe doit être accessible autant sur votre navigateur que sur votre ordinateur, votre téléphone portable ou votre tablette, et ce indépendamment des marques et logiciels.

La disponibilité hors ligne : Le gestionnaire de mots de passe doit être accessible en tout temps, même en l'absence d'une connexion internet. Même si aujourd'hui, la plupart de nos activités se font sur internet, il reste des appareils, des comptes ou des fichiers hors ligne. Comme l'administrateur de votre boîte internet, le mot de passe de votre ordinateur, un fichier crypté, etc.

La fonctionnalité de génération de mots de passe : Le gestionnaire de mots de passe doit offrir une fonctionnalité de génération de mots de passe. L'humain n'est pas bon en génération, même si nous nous trouvons originaux, nous sommes souvent dans des variantes du même mot ou suite de chiffres. Cela étant normal, un bon générateur va fournir un mot de passe généré et paramétrable sur la longueur et la complexité pour être compatible avec le maximum de services et logiciels.

La synchronisation : le gestionnaire doit permettre de se synchroniser entre vos appareils pour que le tout soit à jour. Cela peut être fait par leur technologie ou en passant par un service infonuagique tel qu'iCloud ou OneDrive.

Bonus (j'avais dit 5, mais ce dernier est un game changer si vous l'avez)

L'authentification à deux facteurs : Beaucoup de sites commencent à demander ce genre d'authentification, souvent on va passer par des services tels que Google Auth, mais ce dernier ne peut être synchronisé et il est juste disponible sur mobile.

Alors, si votre gestionnaire offre ce service et qu'il est accessible dans toutes les versions, ceci est un gage de qualité.



Jean-Daniel Genest

En étant Développeur Back-End et expert en cybersécurité, je conçois le squelette et mets en relation l'aspect technique et l'aspect visuel des sites. Avec mon baccalauréat en technologies de l'information, j'ai comme mandat de faire vivre les données brutes en données utilisables, tout en faisant en sorte que le produit final soit rapide, sécuritaire et intègre.

En savoir plus sur moi : <https://jdenest.site/about>

Cette page est pour vous.

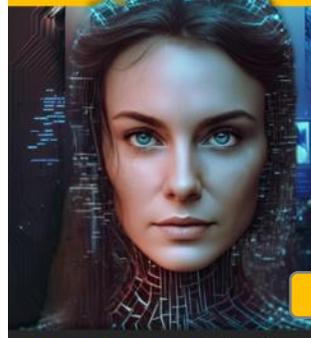
Partagez-nous
une chronique,
une astuce, une info,
ou
autre chose...

Chronique : 400 mots max

Astuces : 150 mots max

Infos : 150 mots max

Soyez en avance sur le futur



Utilisez **ChatGPT**
pour votre
gestion de crise



[Inscrivez-vous ici](#)

La puissance de l'intelligence artificielle à votre service

5 scénarios de gestion de crise

Plongez dans l'univers de la simulation
de gestion de crise

<https://www.crise-resilience.com/simulation>

SCÉNARIO 1 : Cyberattaque de type rançongiciel

SCÉNARIO 2 : Chaîne d'approvisionnement

SCÉNARIO 3 : Catastrophes naturelles

SCÉNARIO 4 : Conflits sociaux

SCÉNARIO 5 : Vol de données

Télécharger les scénarios ici



Les "Pirates seniors" en grève !

Quand les hackers mécontents jettent l'ancre face à la réforme des retraites.

ARTICLE D'ANNE HONYM

Samedi, 1 avril 2023 00:01

MISE À JOUR Samedi, 1 avril 2023 00:75

Le gouvernement a décidé de s'attaquer à un dossier épineux : la réforme des retraites. Mais ce qu'il n'avait pas prévu, c'est que même les hackers les plus chevronnés se rebellent face à cette décision.

Les "Pirates seniors", un groupe de cyberactivistes d'un certain âge ont décidé de jeter l'ancre et de mettre leurs compétences en veille pour une durée indéterminée.

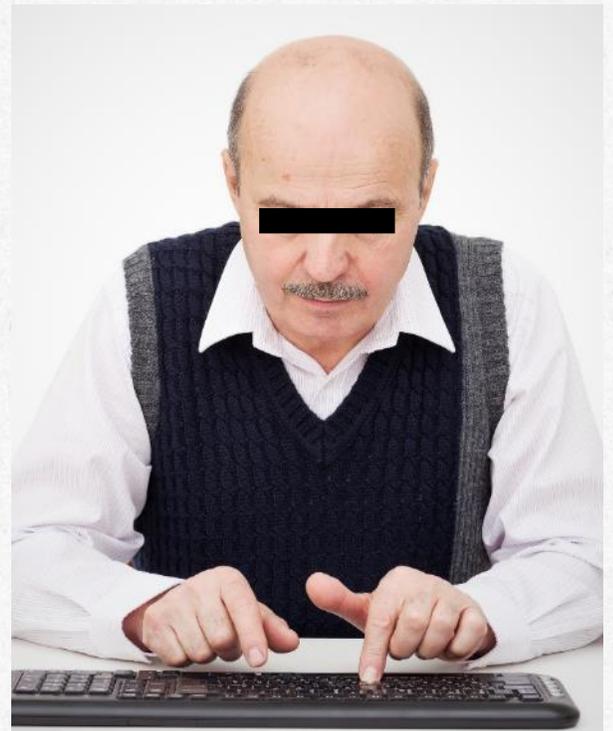
Dans un monde où les nouvelles technologies évoluent à la vitesse de la lumière, ces hackers expriment leurs craintes quant à leur avenir professionnel et leur qualité de vie.

Plongée dans un univers où claviers, codes secrets et arthrite se mêlent pour donner naissance à une contestation inédite.

Les "Pirates seniors", ont choisie de mettre leurs compétences en sourdine et de faire grève pour une durée indéterminée. La cause ?

La réforme des retraites qui les condamne à travailler jusqu'à ce que leurs doigts soient crochus et leurs yeux fatigués. Cette mobilisation inédite prouve que même les cyberactivistes ne sont pas à l'abri des méfaits du gouvernement.

Gérard, 55 ans et toujours prêt à pirater des systèmes avec l'enthousiasme d'un débutant, ne cache pas son désarroi : "J'ai l'impression que l'on veut nous transformer en zombies du clavier. Il n'y a pas de retraite paisible à l'horizon pour les hackers comme moi. Pourtant, je rêvais de troquer mon écran contre une canne à pêche..."



GÉRARD X "Il n'y a pas de retraite paisible à l'horizon pour les hackers comme moi. Pourtant, je rêvais de troquer mon écran contre une canne à pêche..."



ODETTE Y "À ce rythme, je vais devoir déchiffrer des codes secrets en braille !"

De son côté, Odette, 50 ans et reine de la cryptographie, se demande si elle devra apprendre à tricoter avec des mains arthritiques : "C'est comme si on nous demandait de courir un marathon avec des chaussures en béton. À ce rythme, je vais devoir déchiffrer des codes secrets en braille !"

Ces "Pirates seniors" ne sont pas les seuls à se mobiliser contre la réforme des retraites. Raymond, 61 ans et informaticien aguerri, en appelle à la solidarité de tous les claviers : "Nous devons unir nos forces pour faire entendre notre voix. Que vous soyez un hacker aguerri ou un simple utilisateur de clavier, il est temps de dire stop à cette réforme qui nous condamne à taper sur des touches jusqu'à ce que mort s'ensuive."

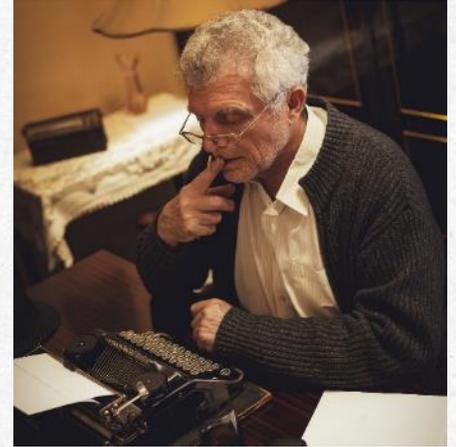
La grève des "Pirates seniors" témoigne de l'ampleur de la contestation face à la réforme des retraites. En levant le pavillon noir et en déposant leurs claviers, ces hackers espèrent faire résonner leur mécontentement jusque dans les couloirs du pouvoir. Reste à savoir si le gouvernement saura décrypter le message de détresse de ces cyberactivistes fatigués, avant qu'ils ne soient contraints de remplacer leurs écrans par des loupes et des cannes blanches.

Intergénérationnel : Les "Cyber-Seniors" se mobilisent pour renforcer la cybersécurité

À l'heure où les cyberattaques se multiplient, un groupe de seniors passionnés d'informatique a décidé d'unir ses forces pour lutter contre les menaces en ligne. Ces "Cyber-Seniors" mettent à profit leur expérience et leur savoir-faire pour protéger les données personnelles et les systèmes informatiques.

Forts de leur longue carrière dans le secteur de l'informatique, ces retraités chevronnés travaillent en étroite collaboration avec des experts en cybersécurité pour déjouer les pièges tendus par les cybercriminels.

Qui a dit que les seniors étaient dépassés par les nouvelles technologies ?



Les techniques proposées par nos cyber-seniors sont d'une efficacité redoutable.



Une révolution, les antivirus actuels seront bientôt dépassés. Ces chiens sont l'avenir de la cybersécurité.

Innovation : Des universités forment des chiens renifleurs de cyberattaques pour renforcer la sécurité en ligne

Dans un monde où les menaces informatiques sont omniprésentes, des chercheurs et des universités ont décidé d'innover pour renforcer la cybersécurité. En s'inspirant des chiens renifleurs utilisés par les forces de l'ordre, des programmes de formation ont été mis en place pour entraîner des chiens à détecter les cyberattaques.

Ces animaux, dotés d'un odorat exceptionnel, sont capables de percevoir les signaux électromagnétiques émis par les appareils électroniques compromis. Ces chiens, baptisés "Cyber-Clebs", sont entraînés à repérer les signes d'intrusion informatique et à alerter leurs maîtres en cas de menace potentielle.

Grâce à cette approche novatrice, les experts en cybersécurité peuvent identifier plus rapidement les failles et les attaques, et ainsi protéger efficacement les systèmes informatiques.

Les "Cyber-Clebs" prouvent que la coopération entre l'homme et l'animal peut jouer un rôle crucial dans la défense de notre monde numérique.

Hélas l'expérimentation avec les chats a été un échec.

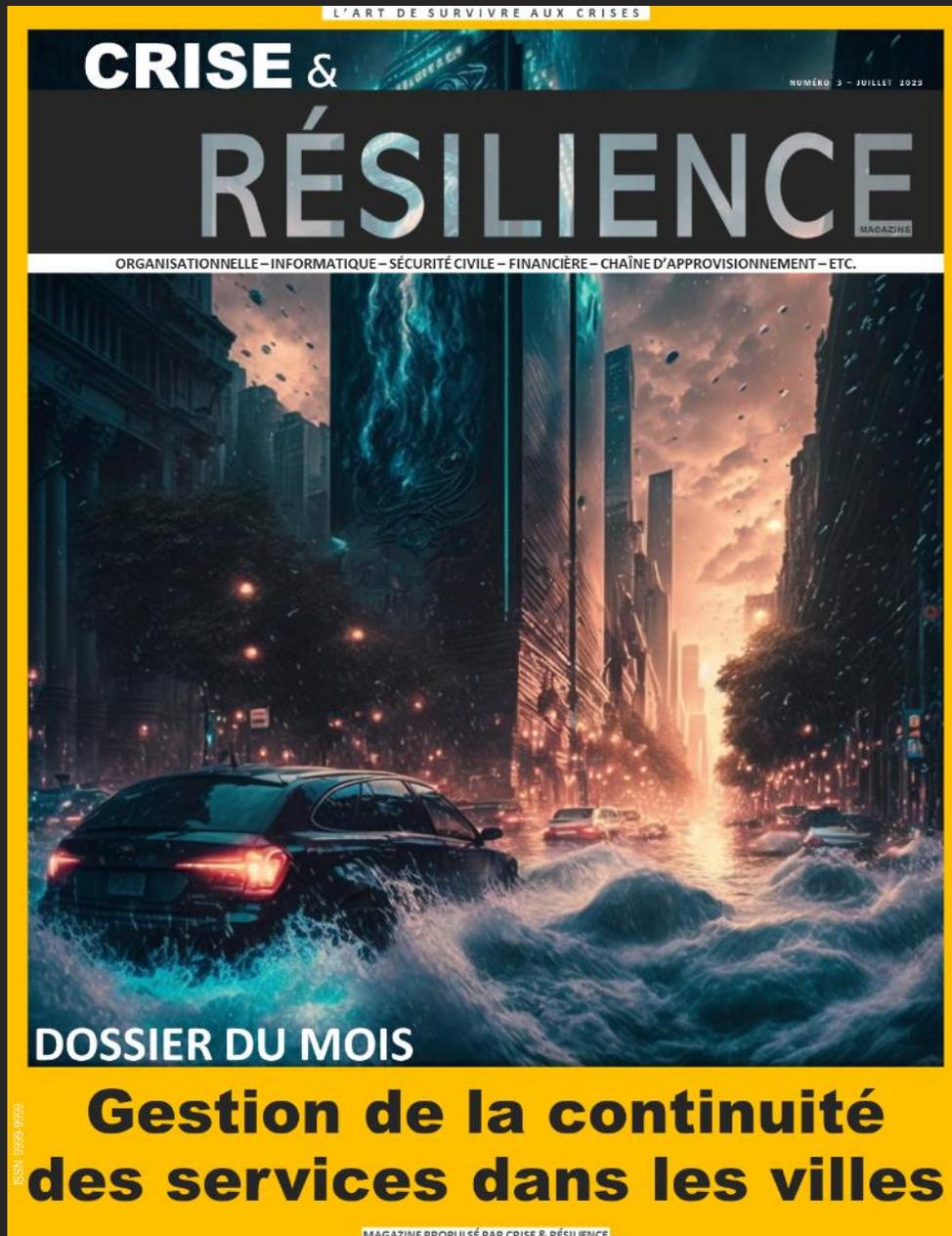
Poissonnerie SANS OS



OFFRE DE LA POISSONNERIE « SANS OS » : Ne manquez pas notre promotion spéciale "Poisson d'avril" ! Pour célébrer cette journée de la plaisanterie et du rire, nous vous proposons une réduction exceptionnelle : tous nos poissons sont gratuits ! 🐟 Et gratuit c'est pas cher!

NE RATEZ PAS LE PROCHAIN MAGAZINE

Prochain numéro le 3 Juillet 2023



Abonnez-vous
pour recevoir le
prochain magazine

www.Crise-Resilience.com/magazine