CRISE & RÉSILIENCE MAGAZINE

Les auteurs des articles sont de

NUMÉRO 4 – OCTOBRE 2023

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

La crise, un outil d'influence
plus qu'une réalité objective

Contrôler son émotion...
...attention à la surcrise

Gestion de la continuité
vue par le corps policier

Assurance Cyber
les éléments clés de la résilience

Avec le DORA,
explorez la résilience de votre entité financière

MARRAINE DE CE NUMÉRO

CÉCILE WEBER

INTERVIEW :
L'IMPORTANCE DU RÔLE DE RESPONSABLE DE CONTINUITÉ D'ACTIVITÉ.

Outil du mois

DOSSIER DU MOIS

Comment mettre en place votre plan de continuité

ISSN 9999-9999

✸ Invitation à Partager Votre Expertise ! ✸

Chers experts en continuité des activités, gestion de crise, résilience organisationnelle, reprise informatique, communication de crise, intelligence économique, sécurité civile, gestion des risques, cybersécurité et autres domaines connexes,

Nous vous invitons chaleureusement à partager votre savoir, vos expériences et vos insights en contribuant à notre magazine dédié à la résilience, la gestion de crise et l'anticipation stratégique. C'est une opportunité unique de mettre en lumière vos connaissances et d'inspirer nos lecteurs en quête de solutions innovantes et de stratégies éprouvées dans ces domaines cruciaux.

Pourquoi Contribuer ?

🚀 Valorisez votre Expertise : Faites reconnaître votre savoir-faire et votre expérience dans les domaines variés de la résilience et de la stratégie.

🌐 Élargissez votre Réseau : Connectez-vous avec d'autres professionnels et experts du secteur.

▨ Éduquez et Inspirez : Aidez les organisations à naviguer et à prospérer dans un environnement incertain et complexe.

Comment Participer ?
Envoyez-nous un résumé de votre proposition d'article à **info@crise-resilience.com**. Les sujets tels que la continuité des activités, la gestion de crise, la communication de crise, l'intelligence économique, la sécurité civile, la gestion des risques, et la reprise informatique sont particulièrement les bienvenus.

Nous avons hâte de découvrir vos perspectives uniques et vos approches novatrices pour renforcer la résilience et la gestion de crise dans le monde professionnel.

Au plaisir de collaborer avec vous pour enrichir et éclairer notre communauté !

Cordialement,

Alexandre Fournier
Directeur de la publication

EDITO DE CÉCILE WEBER

Cécile Weber
Responsable Continuité et Gestion de crise majeure pour le Groupe MAIF.

Vice-Présidente du Club de la Continuité d'Activité.

Je suis très heureuse et honorée d'être la marraine de ce nouveau numéro de Crise & Résilience, encore une fois très riche en contenu.

C'est avec plaisir, que j'ai partagé, au cours d'une interview, avec Alexandre Fournier, mon expérience sur la fonction de Responsable PCA mais également mon analyse sur l'évolution de ses compétences. En effet, pour pouvoir s'adapter à l'évolution des menaces et du caractère plus systémique des crises, le RPCA doit désormais disposer de nouvelles capacités telles que le pragmatisme, la curiosité ou encore la flexibilité mentale et s'entourer également aujourd'hui d'une équipe pluridisciplinaire.

Je vous propose également un article où j'évoque les enseignements de la crise COVID, et notamment la nécessité de renouveler notre approche classique de résilience. Face à l'hypercomplexité des crises, il s'impose à nous de faire évoluer le PCA pour le rendre beaucoup plus flexible. Enfin, je vous partage ma conviction profonde que face à l'ensemble de ces modifications, la résilience individuelle doit désormais glisser vers une résilience beaucoup collective, faite de solidarités nouvelles et de ponts d'efficacité.

Après l'article du mois, très riche, d'Alexandre Fournier et Karine Maréchal Richard sur la méthodologie de mise en place d'un PCA, vous trouverez également dans ce numéro des partages d'expérience ou encore des réflexions sur la distinction entre crise et situation d'urgence, sur le contrôle de ses émotions en gestion de crise, le rôle essentiel de la communication de crise ou encore les exigences réglementaires DORA en matière de résilience opérationnelle numérique et enfin les conseils pour la gestion des crises cyber.

Autant de réflexions et de conseils précieux pour organiser son dispositif de résilience.

Pour conclure, je vous partagerai une phrase de Louis Pasteur que j'affectionne particulièrement

« **La chance ne sourit qu'aux esprits bien préparés** ».

Bonne lecture à tous!

sommaire

Numéro 4 – OCTOBRE 2023

Vous souhaitez rédiger un article!
Contactez-nous sur info@crise-resilience.com

ÉDITO DE LA RÉDACTION

Chers lecteurs et passionnés de la gestion de crise et de la résilience,

C'est avec un immense plaisir et enthousiasme que nous vous présentons le quatrième numéro de notre magazine, dédié à l'art de surmonter l'inattendu. Votre engouement et vos retours positifs sont nos plus grandes récompenses, et ils nous motivent à continuer notre mission de vous offrir des contenus de qualité et d'actualité. Dans le dossier de ce numéro, nous explorons la mise en place d'un plan de continuité des activités. Un dossier complet qui devrait vous faciliter la vie.

Nous tenons à remercier du fond du cœur notre marraine et les auteurs des articles qui nous font confiance. Un immense merci! C'est un réel plaisir de vous côtoyer. Merci pour vos partages et votre temps.

Que ce numéro vous inspire et vous guide dans la construction d'un futur plus sûr et résilient.

Alexandre et Karine

Direction de la publication: Alexandre Fournier – Correction: Véronique Cyr – Création graphique: Alfo65 – Crédit photo: FreePix – Dall-E 3 - Édition: **Crise&Résilience**-1624, rue de la Carrière-Vézina, Québec (Qc), Canada

Dépôt légal: en cours – Numéro ISSN: en cours

CRISE &

RÉSILIENCE C'EST... AUSSI

Une chaîne YouTube avec...

Des interviews d'experts :

Des réponses à vos questions :

Des conférences et formations gratuites

S'ABONNER ici

Une page LinkedIn avec...

Des billets d'actualités, des guides, des astuces, de l'humour, des articles... et pleins d'autres surprises...

Rejoignez-nous sur LinkedIn

NE RATEZ PAS LE PROCHAIN MAGAZINE

Prochain numéro le 8 Janvier 2024

Abonnez-vous

pour recevoir le prochain magazine

www.CriseEtResilience-Magazine.com

L'importance du rôle de responsable de continuité d'activité

Interview

Cécile Weber

Responsable continuité des activités et gestion de crise Groupe MAIF

Vice-Présidente du Club de la Continuité d'Activité (CCA)

Dans une ère dominée par les incertitudes, la maîtrise de la gestion de crise et de la continuité des activités sont devenues impératives pour les organisations.

Cécile Weber, forte d'une riche expérience et reconnue comme une experte en gestion de crise et continuité des activités, dévoile ses réflexions et son expertise sur les fonctions du Responsable du plan de Continuité des Activités (RPCA).

Plongez dans le monde de la gestion de crise et de la continuité des activités et enrichissez vos connaissances avec les points saillants de cette interview.

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.

Au fil de notre entretien, Cécile Weber explore les divers aspects et la complexité inhérente du rôle de Responsable de du Plan de la Continuité des Activités (RPCA).

Cécile met en évidence l'importance de l'autonomie, de la vision stratégique, et de la capacité à maintenir l'objectivité et l'équilibre dans des situations de crise. Elle nous invite à comprendre le monde délicat de la gestion de crise et de la continuité des activités.

Préparez-vous à plonger dans cette conversation enrichissante avec Cécile Weber et à acquérir des connaissances précieuses pour naviguer dans le monde complexe de la gestion de crise et de la continuité des activités.

> **“ L’autonomie et l'objectivité du RPCA sont des piliers pour une gestion de crise saine et efficace. ”**
>
> *Cécile Weber*

Q : Quelle est l'importance du rattachement et des fonctions du RPCA dans la gestion de crise?

R : Cécile souligne que le RPCA doit être autonome et indépendant des Directions Métiers, DRH et DSI. Ainsi son rattachement à une direction des risques indépendante est tout à fait logique.

Le RPCA, selon Cécile, occupe une position déterminante, en cas de crise. Aux côtés de la Direction générale, il va l'alerter puis la conseiller pour déclencher le dispositif de crise puis ,si nécessaire le PCA, en fonction des enjeux de continuité opérationnels pour l'entreprise dans chaque crise.

Q : Quelles compétences et qualités sont indispensables pour un RPCA ?

R : Cécile Weber met en lumière l'importance pour un RPCA de posséder une vision stratégique affinée et une profonde compréhension des enjeux de l'entreprise.

Elle souligne la nécessité de pragmatisme, d'une solide capacité d'adaptation, d'anticipation et d’excellentes qualités relationnelles avec l'ensemble de la chaîne hiérarchique. Cécile parle également d'une certaine solitude sur le sujet, caractéristique du rôle de RPCA, dans toutes les entreprises.

Elle conseille aux RPCA d'échanger et de partager leurs expériences et connaissances avec leurs pairs, en participant à des clubs ou des regroupements de professionnels, permettant ainsi un enrichissement mutuel et une montée en compétence sur les sujets communs. Ces interactions sont essentielles pour découvrir d'autres enjeux et pratiques, même en dehors de son secteur d'activité et ainsi renforcer l’efficacité du dispositif.

Q : Quels sont les principaux défis rencontrés par un RPCA ?

R : Un des défis majeurs pour le RPCA est, l'évaluation objective des signaux faibles et des enjeux pour l'entreprise, pour identifier le moment précis où il va conseiller à la Direction générale d'activer le plan de gestion de crise majeure et le PCA. Cette proposition est lourde de conséquences puisqu'elle signifie un changement radical dans le fonctionnement de l'entreprise.

Cécile partage également son vécu et ses apprentissages durant la crise sans précédent du COVID-19. Elle souligne combien cette période a révélé l’importance de l'adaptabilité et de l'apprentissage continu pour les RPCA. Les leçons tirées de la gestion de cette crise mondiale ont mis en lumière la valeur inestimable des échanges entre pairs, permettant une amélioration continue des stratégies et des plans de continuité des activités.

Découvrez Plus et Plongez Plus Profondément

Cet article ne représente qu'un aperçu des éclairages précieux et de la sagesse de Cécile Weber.

Pour une exploration plus approfondie et pour enrichir vos connaissances dans le monde de la gestion de crise, cliquez sur l’image de la vidéo pour visionner l’interview intégrale.

N'oubliez pas de vous abonner pour rester informé des dernières perspectives et innovations dans ce domaine crucial !

Interview complète de Cécile Weber

Cliquer sur l’image

S’ABONNER ici

Q : Comment devrait être composée l'équipe PCA ?

R : L'équipe PCA doit avoir des profils diversifiés et complémentaires. Une collaboration et une synergie entre ces différents membres de l'équipe sont désormais cruciales pour une gestion de crise holistique et intégrée. Les membres de l'équipe doivent travailler de concert, en mettant en commun leurs expertises respectives pour identifier les meilleures stratégies de réponse et pour élaborer des plans de continuité d'activité robustes et efficaces.

La cohésion de l'équipe PCA est un autre aspect que Cécile juge important. Cette cohésion d'équipe a un sens vraiment particulier en gestion de crise, pour affronter ensemble l'incertitude.

> " La diversité et la complémentarité des compétences sont les pierres angulaires d'une équipe PCA réussie. "
>
> *Cécile Weber*

Q : Quels conseils donneriez-vous pour une équipe PCA restreinte ?

R : Selon Cécile, les équipes restreintes doivent prioriser une approche pragmatique et concentrée. Il s'agit de maximiser l'efficacité et la rapidité dans l'élaboration et la mise en œuvre du PCA, en concentrant les efforts sur les aspects les plus cruciaux et en simplifiant les processus pour garantir une mise en œuvre fluide et efficace en cas de crise. Elle souligne l'importance d'être réalistes quant aux objectifs et aux capacités de l'équipe, et de mettre en place des solutions pratiques et réalisables.

Elle recommande d'adopter une approche pragmatique, en se concentrant sur les éléments les plus essentiels du PCA. Pour Cécile, l'efficacité est primordiale : les équipes doivent définir des priorités claires, assigner les tâches de manière judicieuse et assurer un suivi régulier des progrès.

La formation continue et le partage d'expériences avec d'autres professionnels du domaine sont également cruciaux. Cette démarche non seulement renforce les compétences de l'équipe, mais permet aussi de rester à jour sur les meilleures pratiques dans le domaine de la gestion de crise.

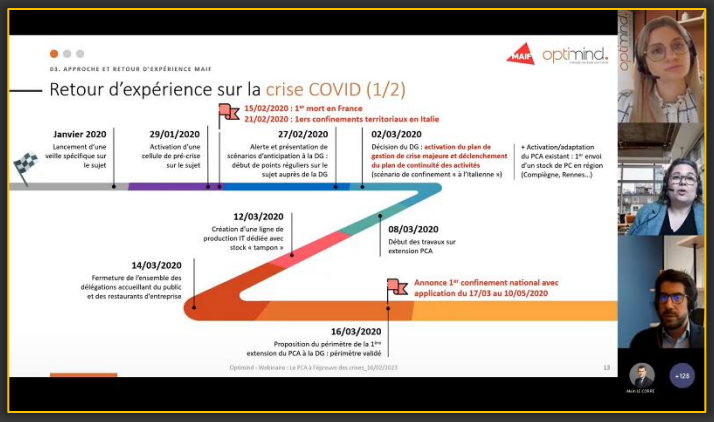
Enfin, Cécile insiste sur la flexibilité, la capacité de s'adapter rapidement aux changements, et l'importance d'une allocation optimale des ressources pour assurer la continuité des activités critiques de l'entreprise.

Interview vidéo réalisée par Alexandre Fournier

Découvrez la chaîne YouTube de Crise et Résilience!

S'ABONNER ici

Retour d'expérience sur la crise Covid avec Cécile Weber



Livre de Cécile Weber

Plan de continuité d'activités

Visitez-le

Club de la continuité d'activité

CCA
Club de la Continuité d'Activité

Dirigeants, élus, responsables,
le poids de l'incertitude pèse-t-il sur vos épaules ?

Nous sommes ici pour transformer vos inquiétudes en plans d'action.

De la gestion de crise à la continuité des opérations, en passant par la reprise informatique en cas de cyberattaque, nous offrons des solutions sur mesure pour rendre votre organisation, qu'elle soit publique ou privée, plus résiliente.

Imaginez votre organisation résiliente, structurée, prête à affronter toute situation imprévue avec confiance.

Anticipez,

ne laissez pas la crise vous surprendre.

Contactez-nous maintenant

Info@crise-resilience.com

Le PCA après la crise du COVID, quels enseignements?

Face à la crise du COVID-19, le télétravail s’est imposé comme solution clé dans les Plans de Continuité d'Activité (PCA), redéfinissant la résilience organisationnelle. Dans ce contexte, les entreprises doivent repenser leurs PCA pour les rendre plus flexibles et adaptatifs, tout en adoptant une approche de résilience collective, essentielle pour naviguer dans l'ère des crises hypercomplexes.

par Cécile WEBER

Responsable continuité des activités et gestion de crise Groupe MAIF

Vice-Présidente Club Continuité Activité

Télétravail, un nouveau mode de travail

Quand on parle enseignements du COVID, le premier bouleversement, très opérationnel est la nouvelle place du télétravail au cœur des modalités de travail dans les organisations, depuis 2020. Ce nouveau mode d'exercice du travail, désormais largement déployé, se retrouve depuis, très naturellement, au cœur du PCA, comme solution de continuité centrale, face au scénario d'indisponibilité des bâtiments.

Rapidement intégré dans les entreprises, le télétravail, a, très logiquement, permis à de nombreuses entreprises de réinterroger leur besoin de site de repli physique, dans le cadre du PCA. Dans une logique de coût évidente, nombreuses ont été celles à abandonner purement et simplement leurs sites de repli physique, et ce, très rapidement, en sortie de la crise COVID. D'autres, ont réduit le périmètre de leur site de repli physique pour ne viser que la reprise d'activités vitales non « télétravaillables » ou encore pour se prémunir de risques liés à la qualité voire à la défaillance des connexions à distance.

L'émergence d'une approche méthodologique renouvelée du PCA face à la mutation des crises

La crise du COVID a parfaitement mis en lumière les nouvelles caractéristiques des crises d'aujourd'hui et de demain. Les entreprises évoluent désormais dans un contexte troublé, confrontées à des situations de crise de grande ampleur, se succédant en diversité et en complexité. On peut parler de mutation des crises.

Les gouvernances doivent prendre conscience du caractère désormais systémique des crises pouvant potentiellement projeter les entreprises vers des situations de rupture avec des risques de perte d'ancrage.

Les acteurs de la continuité se trouvent désormais confrontés à des situations de plus en plus atypiques, potentiellement en rupture avec ce qu'ils connaissaient.

Si nous évoluions encore hier dans un environnement plutôt stable avec des risques plutôt bien identifiés,

l'équation
« un risque = une réponse »
ne semble désormais plus tout à fait adaptée,

tant les caractéristiques des crises (ampleur, caractère systémique, complexité, effets dominos, inadéquation des solutions de continuité ..) les rendent hypercomplexes, voire peuvent les faire basculer vers des crises « hors cadre » .

Cette hypercomplexité bouleverse profondément notre approche de résilience classique et impose d'aborder le PCA différemment. Il s'agit désormais d'évoluer vers un PCA le plus flexible possible, pour qu'il demeure une réponse pertinente face à ces nouvelles crises.

C'est pourquoi, il semble essentiel de se tourner rapidement vers une approche « boîte à outils » du PCA. Il s'agit de prendre comme postulat de départ que le PCA fournit un éventail de solutions de continuité, parfaitement opérationnelles et qu'il conviendra, le jour J, de sélectionner, voire de combiner, en fonction des caractéristiques de la crise rencontrée, afin d'obtenir la ou les solutions de continuité les plus pertinentes pour répondre aux enjeux de continuité de l'entreprise.

"Face aux nouvelles crises de demain, la résilience individuelle devra impérativement passer par une résilience plus collective."

Cécile Weber

Cette démarche adaptée du PCA, doit en amont, impérativement être partagée à la fois avec la gouvernance de l'entreprise mais également avec les opérationnels, afin que chaque partie prenante intègre cette nécessaire adaptation de la méthodologie.

A chaque crise, cette nouvelle étape d'analyse des caractéristiques de la crise et des besoins de l'entreprise devra s'imposer, et être refaite au gré de l'évolution de la crise (crise longue, effets dominos…) pour que la réponse de continuité évolue si besoin pour être toujours au plus près des caractéristiques de la crise.

On mesure donc combien aujourd'hui les aptitudes de pragmatisme, d'adaptation sont désormais au cœur même du dispositif de résilience des entreprises.

“Cette hypercomplexité bouleverse profondément notre approche de résilience classique et impose d’aborder le PCA différemment.”

Cécile Weber

Une approche globale nécessairement plus prospective et plus collective demain

Au-delà des nouvelles caractéristiques des crises, il apparait nécessaire également de s’ancrer dans une approche beaucoup plus prospective et plus collective.

Face aux changements majeurs qui s’imposent à nous, à la fois en force et en nombre (environnementaux, technologiques, sanitaires, économiques, politiques, géopolitiques …), l’adaptation de nos dispositifs doit se faire quasiment en permanence (nouvelles activités, nouvelles interdépendances, nouveaux risques exposant directement ou indirectement l’entreprise…). Face à cette dynamique, il est important d’anticiper et de regarder encore plus loin.

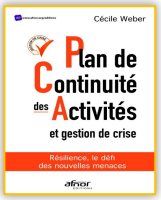
Il ne s’agit pas de prédire mais de s’orienter résolument vers une stratégie d’adaptation encore plus poussée, comme notamment entraîner sa capacité d’étonnement en acceptant de se projeter vers des univers aujourd’hui encore inconnus au travers de modélisation de scénarios beaucoup plus complexes, atypiques par leur ampleur et/ou leur complexité (dépendances complexes, cluster de risques…).

Enfin, face au caractère de plus en plus systémique des crises, je suis convaincue, depuis de plusieurs années, que la résilience des organismes, unitaire et isolée doit laisser place, dès demain, à une approche résolument plus collective, composée de coopérations globales (notamment sur son territoire) et de solidarités nouvelles et innovantes.

Cette approche plus collective implique de créer du partage, des ponts d’efficacité sur un territoire, sur un secteur économique pour aller vers plus de performance. Face aux nouvelles crises de demain, la résilience individuelle devra impérativement passer par une résilience plus collective.

Cécile Weber est Responsable continuité des activités et gestion de crise Groupe MAIF et Vice-Présidente Club Continuité Activité.

Cécile est l’auteur du livre « Plan de Continuité des Activités et gestion de crise, qui a reçu la médaille de l’Académie des Sciences Commerciales.



Cécile est aussi la vice-présidente du Club de la Continuité des Activités.

Depuis 2007, le Club de la Continuité d’Activité (CCA), est un acteur majeur et incontournable de la Continuité d’Activité et la Gestion de Crise.

Le CCA est un réseau d’échanges et de veille qui permet de parfaire ses connaissances, de comparer, conforter et orienter ses choix en matière de Continuité d’Activité et Gestion de Crise. Visitez le site du CCA en cliquant sur l’image ou allez à l’adresse : https://www.clubpca.eu/

Découvrez la chaîne YouTube de Crise et Résilience!

S’ABONNER ici

Formations 2023

Formation lors des 9-10-11-12 octobre 2023!

▼ Aller aux formations en anglais ▼

Sécurité 101-102-103

Formation unique créé par la communauté du Hackfest! Nos formations d'introduction à divers éléments essentiels de sécurité informatique.

CETTE FORMATION EST COMPLÈTE

- Inscription ici

Sécurité Physique 101 (Blue Team), 201 (Red Team), 202 (Rétro-ingénierie) - Français

Formation unique pour vos besoins de sécurité physique en entreprise.

- Inscription ici

PowerShell pour l'équipe bleue - Français

3e édition de cette formation unique et exclusive au Hackfest! Cette formation vise à ajouter une corde à l'arc aux personnes désirant sécuriser des organisations, et ce, à l'aide de PowerShell.

CETTE FORMATION EST COMPLÈTE

- Inscription ici

Compétence de base en radio-amateur - Français

L'obtention du certification de compétence de base en radio amateur n'est pas chose facile. La formation comporte une centaine de sujets très variés couvrant l'électronique, les antennes, la règlementation, etc. L'examen compte 100 questions à choix multiples sur une banque possible de près de 1000 questions.

S'initier à la gestion de crise : apprenez, pratiquez et dominez ! - Français

Imaginez l'impact dévastateur d'une crise sur votre entreprise…

Comment réagiriez-vous face à cette menace imminente ? Êtes-vous vraiment prêt à y faire face et à protéger ce que vous avez construit avec tant de passion ? Si l'incertitude vous envahit, alors notre formation exclusive en gestion de crise est la clé de votre réussite.

En seulement 7 heures, plongez-vous dans une expérience d'apprentissage interactive. Nous dévoilerons les secrets de la gestion de crise pour maximiser l'efficacité de votre organisation. Vous développerez une compréhension des mécanismes de la gestion de crise, créerez une équipe solide et définirez clairement les rôles et responsabilités de chacun.

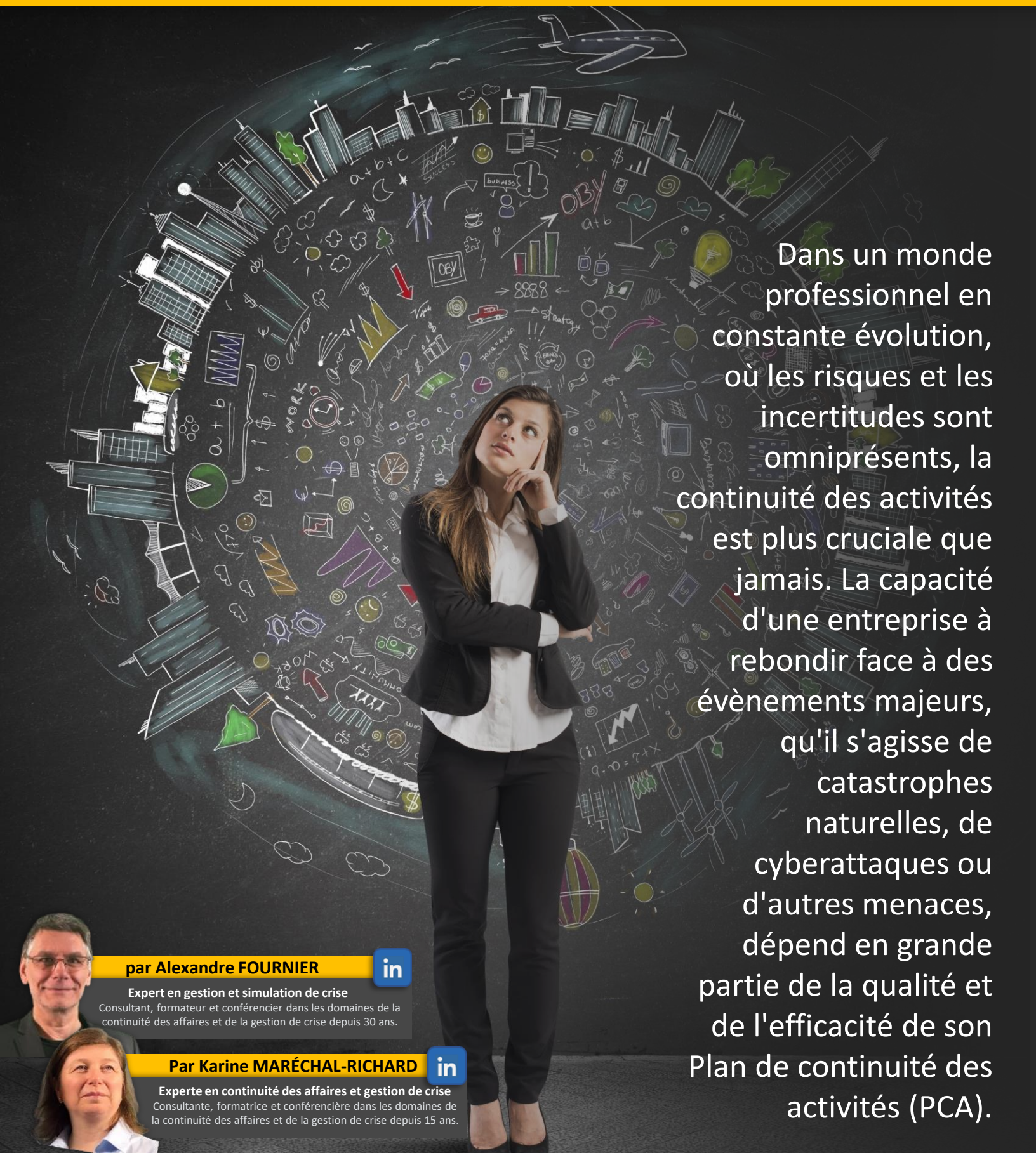
Ensemble, nous irons encore plus loin ! Conscients que la pratique est la clé de la maîtrise, nous vous plongerons dans une simulation de crise réaliste et stimulante en après-midi. Vous mettrez à l'épreuve vos nouvelles compétences et développerez vos réflexes pour affronter les défis qui vous attendent.

À l'issue de cette formation unique en gestion de crise, vous repartirez des connaissances indispensables pour surmonter les obstacles et protéger votre entreprise. Vous maîtriserez les concepts clés pour élaborer un plan solide et efficace.

N'attendez plus ! Inscrivez-vous dès maintenant à cette formation dynamique et pratique et soyez prêt à affronter avec confiance la prochaine crise qui se présentera. Votre entreprise mérite la meilleure protection, et cela commence par vous.

Inscription à la formation

Comment mettre en place un plan de continuité d'activité



Dans un monde professionnel en constante évolution, où les risques et les incertitudes sont omniprésents, la continuité des activités est plus cruciale que jamais. La capacité d'une entreprise à rebondir face à des évènements majeurs, qu'il s'agisse de catastrophes naturelles, de cyberattaques ou d'autres menaces, dépend en grande partie de la qualité et de l'efficacité de son Plan de continuité des activités (PCA).

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.

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.

Un PCA bien conçu n'est pas seulement une assurance contre les aléas; il est le reflet de la vision stratégique d'une entreprise et de sa détermination à assurer sa pérennité.

En garantissant une reprise rapide et efficace en cas de sinistre, il préserve la confiance des parties prenantes, protège la réputation de l'entreprise et assure la stabilité financière.

Ce dossier s'adresse principalement aux dirigeants d'entreprise, aux responsables opérationnels, aux gestionnaires de risques, et à toute personne impliquée ou intéressée par la continuité des activités.

Que vous soyez novice en la matière ou que vous cherchiez à affiner votre approche actuelle, vous y trouverez des orientations précieuses.

Pour la rédaction de ce dossier, nous nous sommes appuyés sur la feuille de route éprouvée que nous déployons lors de la mise en place de PCA pour nos clients.

Cette feuille de route est non seulement alignée sur les normes et les meilleures pratiques en vigueur en 2023, mais elle tire également sa force de près de 30 ans d'expérience multidisciplinaire dans le domaine.

Le but de cette feuille de route est de fournir, à haut niveau, un guide structuré et détaillé pour la mise en place, la réalisation et la validation d'un PCA robuste et efficace.

Elle vise à transformer une tâche potentiellement écrasante en un processus gérable étape par étape, tout en garantissant que chaque élément essentiel soit pris en compte.

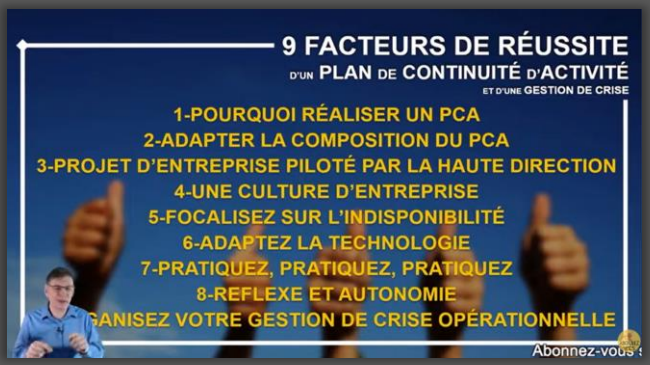
Le document est structuré autour de trois phases principales :

- la première concerne la préparation pour la mise en place du PCA,
- la deuxième s'articule autour de la réalisation proprement dite du PCA,
- et la troisième est dédiée à la validation et à l'amélioration continue du plan établi.

Pour faciliter votre navigation, chaque phase est subdivisée en étapes clés, détaillées et explicitées. Des sous-sections fournissent des recommandations spécifiques, des conseils et des meilleures pratiques pour chaque étape.

Vous êtes invité à suivre cette feuille de route de manière linéaire, bien que certains éléments puissent nécessiter une approche itérative en fonction des besoins spécifiques de votre entreprise.

VIDÉO – 9 facteurs de réussite d’un PCA



10 bénéfices d'un plan de continuité d'activité

- **Résilience et rentabilité optimisées :** un PCA minimise les temps d’arrêt et optimise la gestion des ressources, soutenant ainsi la continuité opérationnelle et la rentabilité.
- **Image de marque renforcée :** la démonstration d’une capacité à maintenir les opérations en cas de perturbation améliore la réputation et la satisfaction client, consolidant ainsi la confiance et les relations à long terme avec les partenaires et les clients.
- **Culture de proactivité :** un PCA incite à une attitude proactive et à l'anticipation des risques, renforçant la cohésion et la réactivité des équipes.
- **Préservation des actifs :** la mise en œuvre d’un PCA protège les ressources et les investissements cruciaux, sécurisant ainsi la valeur de l’entreprise.
- **Gestion efficace des crises :** un PCA permet une réponse ordonnée et rapide à des événements imprévus, minimisant les dommages et perturbations.
- **Réduction des pertes financières :** en minimisant les coûts liés aux interruptions de service, un PCA facilite une reprise rapide des activités et limite les pertes financières.
- **Amélioration continue :** un PCA encourage la réévaluation et l’ajustement réguliers des processus et des stratégies, permettant une optimisation continue et une adaptation aux changements du contexte d’affaires.
- **Assurance de la continuité des services :** le PCA garantit une continuité de service, renforçant ainsi la confiance des clients et des partenaires.
- **Conformité et sécurité :** la mise en œuvre d’un PCA aide à répondre aux exigences réglementaires et à maintenir la sécurité des informations et des données.
- **Engagement et responsabilisation des employés :** un PCA sensibilise et responsabilise les employés sur l'importance de la continuité des activités, favorisant un environnement de travail conscient et engagé.

Cette liste n’est pas exhaustive…

FEUILLE D

10 ÉTAPES POUR FORTIFIER LA S

Réaliser un état des lieux de la situation actuelle

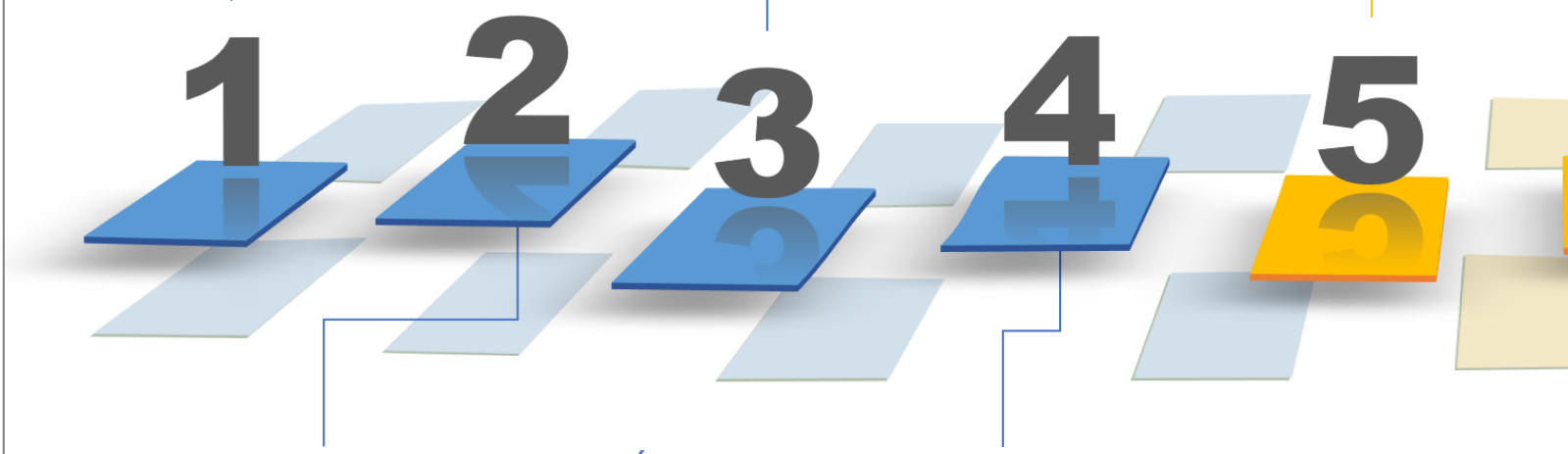
1. Nommer un responsable
2. Réaliser l'état des lieux

Définir les besoins de continuité

11. Répertorier les risques
12. Réaliser l'analyse d'impact (BIA)
13. Présenter l'analyse d'impact (BIA)

Mettre en place les strat

16. Suivre et valider la mise
des stratégies



Démarrer le projet

3. Obtenir l'appui de la direction
4. Déterminer le périmètre
5. Définir les objectifs
6. Déterminer une structure organisationnelle
7. Élaborer un plan de communication
8. Définir la gestion documentaire
9. Rédiger le plan de projet
10. Rédiger une politique de continuité

Élaborer des stratégies de continuité

14. Identifier des stratégies de continuité pour :
    - Relocaliser le personnel
    - Rendre opérationnelle son informatique
    - Pallier l'indisponibilité des employés clés
    - Pallier une défaillance des fournisseurs clés
    - Pallier une indisponibilité des équipements essentiels
    - Minimiser la perte des documents essentiels
    - Maintenir sa trésorerie
    - Définir son organisation de gestion de crise
15. Proposer les stratégies à la direction

Rédiger les p

17. Produire les
18a. Rédiger le
18b. Rédiger le
19. Rédiger le p
20. Produire le
21. Élaborer le

Cliquez sur l'image pour télécharger
cette feuille de route
www.crise-resilience.com/feuillederoutepca

DE ROUTE

URVIE DE VOTRE ORGANISATION

égies
en œuvre

Former et sensibiliser

22. Produire un plan de formation
23. Élaborer un plan de sensibilisation
24. Évaluer le résultat de la formation et de la sensibilisation

Surveiller son PCA

27. Auditer son PCA
28. Définir des indicateurs de performance
29. Réaliser des revues de direction

rocédures et plans

s gabarits
s procédures de continuité métier (PCM)
s procédures de continuité informatique (PCIT)
plan de gestion de crise
plan de communication de crise
plan de retour à la normale

S'entraîner et tester

25. Définir un programme d'exercices
26. Déterminer le processus de réalisation des exercices et des tests

Améliorer son PCA

30. Traiter les non-conformités
31. Actualiser son PCA

CRISE & RÉSILIENCE
L'ART DE SURVIVRE AUX CRISES
crise-resilience.com

PHASE 1 - PRÉPARATION

La phase initiale est essentielle à tout projet d'envergure. Semblable à la fondation solide d'un édifice, cette étape garantit que toutes les actions futures reposent sur une base bien définie et robuste. En évaluant minutieusement la situation actuelle, en identifiant les responsabilités et en définissant les objectifs, vous établissez les prérequis essentiels pour assurer la continuité des activités. Cette phase éclaire votre chemin, éliminant les incertitudes et établissant des paramètres clairs pour les étapes à venir.

Étape 1 : Réaliser un état des lieux de la situation actuelle

Avant de mettre en œuvre un plan ou une stratégie, il est essentiel de déterminer le niveau de résilience actuel de l'entreprise. Cette première étape consiste à évaluer la situation présente, identifier ses points forts et ses faiblesses, ainsi que les ressources à disposition. Cela établit une base solide pour élaborer de futurs plans et garantir qu'ils soient en adéquation avec la réalité opérationnelle.

Tache 1. Nommer un responsable

Avant de débuter un état des lieux, il est impératif de désigner un responsable chargé de mettre en œuvre, maintenir et améliorer le PCA, ainsi que d'animer et conseiller la cellule de crise.

Ce responsable est connu sous le nom de Responsable du plan de continuité des activités (RPCA). Il aura en charge la coordination des actions, la supervision de l'équipe et agira comme intermédiaire avec la direction. Ce rôle demande des aptitudes en gestion de projet, une solide compréhension des opérations de l'entreprise, et une habileté à communiquer efficacement à travers l'ensemble des échelons hiérarchiques.

La nomination du responsable doit être effectuée par un membre de la haute direction, assurant ainsi que le projet bénéficie de l'attention et des ressources adéquates.

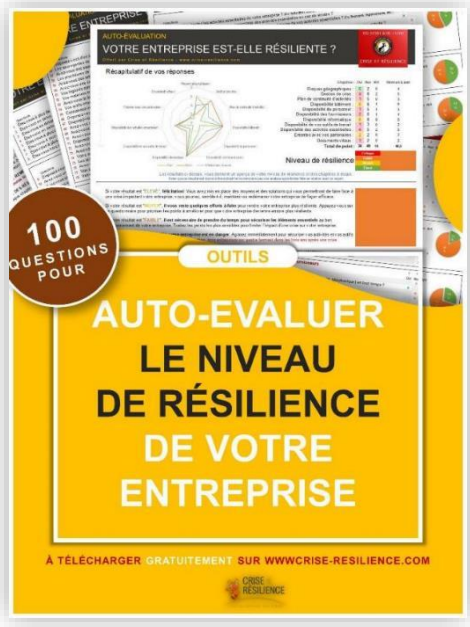
Pour plus d'information sur le profil du responsable, cliquez sur la vidéo

Tache 2. Réaliser l'état des lieux

Une fois le RPCA mandaté, sa première mission est de réaliser un état des lieux exhaustif. Cette démarche fondamentale sert à évaluer la situation actuelle de l'entreprise en commençant par analyser les ressources, y compris les actifs matériels et immatériels, les processus et les compétences du personnel. Parallèlement, une identification rigoureuse des vulnérabilités doit être effectuée à travers une analyse des risques, qui englobe tant les risques naturels que technologiques et humains.

Pour renforcer cette analyse, il est crucial de se pencher sur le contexte externe. Cela implique de décrypter les influences macroéconomiques à l'aide d'une analyse PESTEL(1), d'évaluer les forces et faiblesses des concurrents et de saisir les opportunités et menaces du marché. L'intégration des besoins et attentes des parties prenantes clés, obtenus via des entretiens ou des ateliers, ajoute une couche supplémentaire de profondeur à cette évaluation.

Toutes ces données, combinées à une compréhension des tendances spécifiques au secteur de l'entreprise, permettent de dresser un tableau complet de la situation et d'identifier les domaines nécessitant une attention immédiate. Ce processus holistique garantit un plan de continuité des activités à la fois robuste et adapté au contexte spécifique de l'entreprise.



Cliquez sur l'image pour télécharger l'auto-évaluation

Ou visitez le site www.crise-resilience.com

(1) La méthode PESTEL est un outil d'analyse stratégique qui identifie les facteurs Politiques, Économiques, Socio-culturels, Technologiques, Environnementaux et Légaux pouvant influencer un secteur ou une entreprise. Elle permet d'anticiper les opportunités et menaces du macro-environnement. Cette analyse facilite la prise de décision en contexte d'incertitude.

Étape 2 : Démarrer le projet de continuité des activités

Une fois une vision claire de la situation actuelle, l'étape suivante est de démarrer le projet de continuité. Cela nécessite une approbation et un soutien de la direction, la définition des objectifs précis et la mise en place d'une structure organisationnelle pour le pilotage du projet.

Tache 3. Obtenir l'appui de la direction

Pour assurer le succès d'un projet de continuité des activités, il est impératif d'obtenir le soutien explicite de la haute direction.

Ce soutien doit être matérialisé par une lettre de mandat ou une communication officielle qui attribue les ressources nécessaires et établit le projet comme une priorité organisationnelle

Tache 4. Déterminer le périmètre

Dès le début, il est essentiel de définir clairement le périmètre du projet afin d'éviter toute ambiguïté ou écart ultérieur. Il convient d'identifier les unités opérationnelles, les fonctions et les processus impliqués.

Les critères de sélection peuvent inclure le niveau de criticité pour les opérations de l'entreprise, les obligations légales, ainsi que les attentes des parties prenantes.

Tache 5. Définir les objectifs

Une fois le périmètre établi, des objectifs SMART (Spécifiques, Mesurables, Atteignables, Réalistes, et Temporellement définis) doivent être formulés. Ces objectifs serviront de base pour l'évaluation des performances et l'orientation du projet.

Par exemple, un objectif pourrait être de rétablir les fonctions commerciales critiques dans les 24 heures suivant une panne majeure.

Tache 6. Déterminer une structure organisationnelle

Afin de gérer le projet de manière efficace, une structure organisationnelle doit être établie. Cela comprend la désignation d'un chef de projet, des membres de l'équipe de continuité des activités et la définition de leurs rôles et responsabilités respectifs.

Cette équipe peut être composée de responsables issus des départements comme les finances, les ressources humaines, la technologie de l'information, et la production.

Tache 7. Élaborer une communication projet

Un plan de communication du projet bien structuré est essentiel pour maintenir l'intérêt des parties prenantes du projet. Ce plan doit détailler les modes de communication, les responsables de la diffusion de l'information, et les différentes parties prenantes à informer (employés, partenaires, fournisseurs, etc.).

Le plan doit également préciser les plateformes qui seront utilisées pour la communication, que ce soit par e-mail, intranet de l'entreprise, ou réunions régulières.

Et bien sûr ce plan devra aussi proposer les communications de sensibilisations et leurs rythmes de diffusion.

Tache 8. Définir la gestion documentaire

On ne se mentira pas… la mise en place d'un PCA génère beaucoup de documentation. La manière dont les documents seront gérés tout au long du projet – et post-projet - doit être clairement définie. Cela inclut la création, le stockage, l'accès, et la mise à jour de tous les documents pertinents. Un système de gestion électronique des documents (GED) peut être mis en place pour faciliter ce processus.

À noter :

- Certains documents revêtent un certain niveau de confidentialité qu'il faudra prévoir (chiffrement, distribution, etc.)
- Il faudra pouvoir accéder aux documents opérationnels lors de la crise. Donc, prévoyez dès à présent la possibilité d'accès à ces documents malgré une indisponibilité informatique…

Tache 9. Rédiger le plan de projet

Après avoir recueilli toutes les informations et les données nécessaires, le plan de projet peut être rédigé. Ce plan doit contenir un calendrier précis, un budget détaillé, et des indicateurs de performance clé (KPI) pour suivre le progrès.

Le plan doit être suffisamment flexible pour accueillir des ajustements en cas d'événements imprévus, mais assez rigoureux pour guider l'équipe de projet vers l'atteinte des objectifs.

Tache 10. Rédiger une politique de continuité

La dernière étape consiste à rédiger la politique de continuité des activités, qui est le document directeur intégrant toutes les étapes précédentes.

Cette politique doit être revue et approuvée par la direction et doit être facilement accessible à tous les membres de l'entreprise. Elle devra être mise à jour régulièrement pour s'assurer qu'elle reste alignée avec les besoins changeants de l'entreprise et les meilleures pratiques de l'industrie.

"Sans le soutien actif de la direction, vous vous exposez à consacrer une énergie et un temps excessifs, pour finalement aboutir à des résultats médiocres."

Alexandre Fournier

Étape 3 : Définir les besoins de continuité

Après avoir établi une base solide pour le projet, il est maintenant temps d'identifier précisément quels sont les besoins réels de l'entreprise en matière de continuité.

Cette étape met l'accent sur la reconnaissance des risques (pouvant impacter directement l'entreprise) et la compréhension des impacts qu'ils pourraient avoir. C'est ici que l'on détermine les éléments vitaux de l'entreprise et les exigences pour assurer leur fonctionnement continu.

Tache 11. Répertorier les risques et les scénarios

Une fois qu'un état des lieux a été réalisé, l'étape suivante consiste à inventorier tous les risques susceptibles d'affecter la continuité des activités.

Conformément à la norme ISO 22301, un processus de gestion des risques est indispensable pour identifier, analyser et évaluer les risques. L'analyse de risque présente une perspective complète sur les dangers pouvant entraîner une interruption d'activités.

Toutefois, ces risques varient : catastrophes naturelles, terrorisme, mouvements sociaux, cyberattaques, accidents industriels, espionnage, entre autres.

Il est alors irréaliste de concevoir des plans pour chaque risque, étant donné l'impossibilité de recenser toutes les menaces. C'est pourquoi nous vous conseillons de travailler par scénarios d'indisponibilité.

On en distingue cinq types : indisponibilité bâtiment, informatique, ressources humaines essentielles, fournisseurs essentiels et équipements spécifiques.

L'objectif d'un PCA est de traiter les conséquences d'un sinistre plutôt que ses causes.

En conséquence, le RPCA va concentrer ses efforts sur la mise en place de stratégie de continuité pour réduire les impacts d'un risque.

Le RPCA s'appuiera sur les scénarios identifiés pour réaliser l'Analyse d'Impact sur les Activités (AIA ou BIA en anglais).

Tache 12. Réaliser l'analyse d'impact sur les activités (AIA ou BIA)

L'Analyse d'Impact sur les Activités (AIA) est une évaluation formelle des effets potentiels que les différents types de sinistres pourraient avoir sur les opérations de l'entreprise.

Elle permet de prioriser les activités critiques qui nécessitent une reprise rapide et efficace en cas de crise. Des indicateurs comme le Délai maximal d'interruption admissible (DMIA ou RTO) et la Perte de données maximal admissible (PDMA ou RPO) seront définis pour chaque activité critique. Cette analyse permet ainsi de déterminer tous les besoins en ressources humaines et matériels nécessaires pour maintenir ou reprendre une activité en cas de sinistre.

Cette analyse doit être menée en étroite collaboration avec des responsables de continuité des activités (RCA), experts dans leur domaine et parfaitement familiers avec l'activité, ainsi qu'avec les gestionnaires auxquels l'activité est rattachée, afin de garantir que tous les aspects de l'entreprise soient considérés.

Astuce : Lors de cette réalisation, on peut en profiter pour commencer à rédiger le volet procédure de reprise ou de continuité métiers du département que l'on analyse. Cela fait gagner beaucoup de temps dans la mise en place du PCA et permet de disposer immédiatement de procédure minimale.

Tache 13. Présenter l'analyse d'impact sur les activités

Après avoir réalisé l'analyse d'impact, il est important de la présenter à la direction et aux autres parties prenantes concernées pour validation et approbation. Cette présentation devrait non seulement mettre en évidence les zones de risque et les fonctions critiques, mais également proposer des solutions ou des mesures d'atténuation pour chaque risque identifié.

L'objectif est d'obtenir un consensus sur les priorités et de garantir que les ressources nécessaires seront allouées pour la mise en œuvre des mesures de continuité. Des documents de support, tels que des tableaux, des graphiques et des rapports détaillés, peuvent être utiles pour faciliter la compréhension et la prise de décision.

Cette étape établit les bases pour le développement d'un PCA efficace et pragmatique.

Il est donc essentiel de prendre du temps et des ressources suffisantes à cette phase, pour s'assurer que les actions futures sont à la fois ciblées et efficaces.

Étape 4 : Élaborer des stratégies de continuité

Avec une compréhension claire des besoins de continuité, l'entreprise peut désormais développer des stratégies pour répondre à ces besoins. Ces stratégies couvriront une gamme de scénarios potentiels et fourniront des solutions pour garantir la continuité dans diverses situations. C'est la phase de planification proactive pour prévenir les perturbations.

Note : Lorsque vous êtes accompagné par un expert en PCA, celui-ci devrait vous faire gagner beaucoup de temps, car les stratégies sont souvent les mêmes d'une entreprise à une autre.

Tache 14. Identifier des stratégies de continuité pour :

Relocaliser le personnel

Face à un événement majeur nécessitant une délocalisation, disposer d'un site alternatif opérationnel est essentiel. Les solutions varient entre bureaux temporaires, sites distants de l'entreprise, ou travail à distance. Le choix optimal dépend des tâches, des besoins en équipement, et des délais d'activation.

Pallier l'indisponibilité des employés clés

Identifiez les fonctions vitales et les employés associés pour élaborer des plans de remplacement ou de formation croisée, assurant la continuité des opérations même en l'absence d'individus clés.

Conseil : Maintenez une liste de fournisseurs pouvant déployer rapidement des experts en TI.

Pallier une défaillance des fournisseurs clés

La crise du Covid a démontré les risques d'une dépendance excessive envers un seul fournisseur. Pour atténuer ce risque, diversifiez vos sources d'approvisionnement et établissez des contrats d'urgence avec différents fournisseurs.

Continuité Informatique en Entreprise

La continuité des services informatiques est essentielle pour la survie d'une entreprise. Une stratégie robuste dans ce domaine se concentre sur :

- Aspect Humain : En cas d'incident majeur, la disponibilité des experts en TI est prioritaire. Il est crucial d'avoir un plan pour leur transfert rapide vers un lieu sûr et opérationnel si nécessaire.
- Aspect Technique : Le choix du matériel doit correspondre aux Délais Maximaux d'Interruption Acceptables (DMIA) définis après l'Analyse d'Impact sur l'Activité (AIA). Qu'il s'agisse de serveurs de secours, de centres de données ou de solutions cloud, leur fiabilité doit être testée pour assurer leur performance en crise.

La clé est la préparation. Anticipez les défis et élaborez des plans de reprise pour garantir la continuité des opérations en cas d'incident.

Prévention de la Perte de Documents Clés

Assurez une sauvegarde régulière des documents essentiels et stockez-les dans des lieux sûrs, y compris en ligne. Implémentez un système de gestion documentaire pour une récupération aisée en cas d'urgence. Notez que les plans et procédures du PCA font partie des documents prioritaires.

Définir son organisation de gestion de crise

Créez une unité de décision de crise et une ou plusieurs unités opérationnelles avec des membres assignés pour gérer divers aspects d'une urgence. Élaborez un manuel de gestion de crise fournissant directives et protocoles à respecter.

Pallier une indisponibilité des équipements essentiels

Pour tout équipement vital, planifiez une maintenance préventive, stockez des pièces de rechange et nouez des partenariats avec des services d'urgence pour des réparations express.

Maintenir sa trésorerie

Pour maintenir la trésorerie pendant une période de crise, envisagez de créer un fonds d'urgence, d'ouvrir des lignes de crédit, ou d'avoir des accords financiers flexibles avec vos partenaires.

Tache 15. Proposer les stratégies à la direction

Après avoir identifié et élaboré ces stratégies de continuité et/ou de reprise, la prochaine étape est de les présenter à la direction pour approbation. Cette présentation devrait être accompagnée d'une analyse coût-bénéfice pour chaque stratégie, ainsi que d'un calendrier de mise en œuvre. L'objectif est de s'assurer que les décideurs sont pleinement informés et que l'entreprise peut allouer efficacement les ressources nécessaires pour garantir la continuité des opérations.

Avec c'est 4 premières étapes, vous venez de jeter les bases de votre PCA, un pas crucial pour assurer la continuité de votre entreprise. Tout comme un architecte transforme un terrain vierge en une structure magnifique, vous allez maintenant donner forme à vos analyses et stratégies.

La prochaine étape ? Mettre en place des plans et procédures qui garantissent la résilience de votre entreprise. N'attendez plus, le moment est venu de concrétiser votre vision!

PHASE 2 - RÉALISATION

Après avoir établi les bases nécessaires, cette phase s'articule autour de la mise en action. Vous commencez la transformation de vos plans en initiatives concrètes pour assurer une continuité d'activité. C'est comme un architecte qui passe d'un plan sur papier à une construction réelle.

Étape 5 : Mettre en place les stratégies

Maintenant, il est temps de détailler cette transformation. Élaborez des procédures, formulez des plans stratégiques, et déployez des formations pertinentes pour construire solidement votre PCA. Chaque élément mis en œuvre est le fruit d'une réflexion stratégique, assurant que le PCA est parfaitement adapté à vos besoins.

Tache 16. Suivre et valider la mise en œuvre des stratégies

Une fois que les stratégies de continuité ont été définies et approuvées par la direction, l'étape suivante est de passer à leur mise en œuvre effective. Cependant, la mise en œuvre n'est pas un processus en "pilote automatique"; elle nécessite un suivi rigoureux et une validation continue pour s'assurer que les objectifs sont atteints conformément aux plans établis. Voici quelques points de vigilance :

Établissement de jalons

Définissez des jalons clairs pour chaque stratégie, avec des dates d'échéance spécifiques et des critères mesurables pour évaluer le succès. Cela permet de suivre la progression et d'identifier rapidement toute déviation par rapport au plan.

Allocation des ressources

Un élément crucial de cette phase est d'assurer que toutes les ressources nécessaires (financières, humaines, technologiques) sont disponibles et affectées aux tâches pertinentes. L'efficacité de la mise en œuvre repose souvent sur la capacité à disposer rapidement des ressources nécessaires.

Équipes de suivi

Formez des équipes ou désignez des individus spécifiques responsables du suivi de chaque stratégie. Ces personnes seront chargées de recueillir des données, de suivre les progrès et de signaler les avancements et les obstacles au comité de gestion de projet ou à la cellule de crise.

Évaluation continue

Au fur et à mesure que les stratégies sont déployées, il est essentiel d'évaluer régulièrement leur efficacité. Cela signifie surveiller les progrès, identifier les obstacles potentiels, et apporter des ajustements en temps réel pour assurer que les objectifs de continuité sont atteints.

Documentation

Tenez à jour une documentation complète de la mise en œuvre, y compris les changements apportés au plan original, les raisons de ces changements, et toute communication pertinente. Cette documentation sera précieuse pour les audits et pour l'analyse post-crise.

Validation finale

Une fois que les stratégies sont pleinement opérationnelles, il est crucial de les valider. Cela peut impliquer des tests, des simulations ou d'autres formes d'évaluation pour s'assurer qu'elles fonctionnent comme prévu en conditions réelles. Par exemple, une stratégie visant à relocaliser le personnel peut être testée en organisant un exercice d'évacuation ou une simulation de travail à distance. On en parle plus loin…

La mise en œuvre efficace des stratégies est le noyau de tout plan de continuité.

Plus elle est préparée et partagée, plus cela sera facile.

Étape 6 : Rédiger les procédures et plans

Pour garantir l'efficacité et la reproductibilité des stratégies de continuité, il est essentiel de les documenter sous forme de procédures et de plans. Cette étape vise à assurer qu'en cas d'incident, il existe des directives claires et bien définies pour guider l'entreprise vers une reprise sûre et efficace.

Tache 17. Produire les gabarits

L'élaboration de gabarits solides et cohérents est une étape cruciale pour garantir la continuité des activités. Ces modèles servent de base pour tous les documents ultérieurs, assurant une uniformité dans la présentation et la diffusion de l'information. En disposant d'un gabarit robuste, l'entreprise peut s'assurer que toutes les procédures et tous les plans sont conformes aux normes établies, facilitant ainsi la formation, la compréhension et l'exécution par le personnel.

Tache 18a. Rédiger les Procédures de Continuité Métier (PCM)

Les PCM sont un élément central de toute stratégie de continuité. Elles fournissent un guide détaillé sur la manière dont l'entreprise doit réagir face à des interruptions spécifiques, garantissant que les opérations essentielles se poursuivent ou redémarrent avec le moins de perturbations possible. Ces procédures doivent non seulement détailler les étapes à suivre, mais aussi identifier clairement les responsabilités de chacun.

Astuce : Lors de la tâche 12 « Analyse d'impact de l'activité », il est possible de commencer à rédiger ces procédures

Tache 18b. Rédiger les Procédures de Reprise Informatique (PRI)

Tandis que les PCM couvrent les opérations globales de l'entreprise, les PRI se concentrent spécifiquement sur les aspects informatiques. Elles définissent comment l'entreprise doit répondre à des perturbations technologiques, telles que des destructions de serveur ou des cyberattaques, garantissant que les systèmes informatiques vitaux demeurent opérationnels ou puissent être rapidement reconstruits.

Tache 19. Rédiger le Plan de Gestion de Crise (PGC)

Lorsqu'une crise survient, une action rapide et coordonnée est essentielle. Le plan de gestion de crise fournit un cadre détaillé pour gérer diverses situations d'urgence, en stipulant les responsabilités, en établissant des procédures claires et en définissant les canaux de communication à utiliser.

Voir la vidéo →

Tache 20. Produire le Plan de Communication de Crise (PCC)

La communication est vitale en période de crise. Ce plan doit donc détailler comment, quand et quoi communiquer aux parties prenantes concernées, qu'il s'agisse d'employés, de clients ou de partenaires. Il doit également identifier qui sont les porte-paroles autorisés et quels sont les canaux de communication à privilégier.

Tache 21. Élaborer le Plan de Retour à la Normale (PRN)

Après avoir géré une situation de crise, l'objectif est de ramener l'entreprise à son fonctionnement normal. Ce plan décrit les étapes nécessaires - à haut niveau - pour y parvenir. Attention à ne pas rentrer dans le détail lors de cette tâche.

Étape 7 : Former et sensibiliser

Un plan, aussi bien conçu soit-il, n'est efficace que si les personnes concernées savent comment l'exécuter. Cette étape met l'accent sur la formation des parties prenantes directes du PCA, ainsi que la sensibilisation de l'ensemble des employés à l'importance de la continuité des activités. C'est ici que la théorie rencontre la pratique, en préparant chaque individu à jouer son rôle.

Tache 22. Produire un Plan de Formation (PF)

La formation est cruciale pour assurer que toutes les parties prenantes comprennent leur rôle dans la continuité des opérations. Un plan de formation détaillé devrait être produit, en spécifiant les compétences à développer, les publics cibles, les méthodes pédagogiques à utiliser et le calendrier de déploiement. Le plan doit être flexible afin de s'adapter aux différents niveaux d'interventions et de compétence ainsi qu'aux besoins changeants de l'entreprise.

Tache 23. Élaborer un Plan de Sensibilisation (PS)

Outre la formation, il est vital de sensibiliser tous les membres de l'entreprise aux enjeux de la continuité des activités. Le plan de sensibilisation doit donc inclure des éléments tels que les séances d'information, les newsletters, et même des simulations de scénarios de crise. Le but est de s'assurer que tout le monde est conscient de l'importance de la continuité, comprend les risques associés et sait comment réagir en cas de situation d'urgence.

Tache 24. Évaluer le résultat de la formation et de la sensibilisation

Après la mise en œuvre des plans de formation et de sensibilisation, une évaluation rigoureuse doit être effectuée pour mesurer leur efficacité. Cette évaluation peut inclure des questionnaires, des entretiens, ainsi que des exercices pratiques pour tester les compétences acquises. Les résultats de cette évaluation permettront de faire des ajustements nécessaires aux plans existants et de mieux préparer l'entreprise pour des situations d'urgence futures.

Suite à la Phase 2, votre entreprise s'est dotée d'une base solide pour la continuité des activités. À ce stade, vous disposez de procédures et de plans théoriques. La formation et la sensibilisation des parties prenantes ont permis que chaque individu au sein de l'entreprise comprenne son rôle et la manière de le jouer en cas de perturbation. L'efficacité réelle d'un PCA ne peut être mesurée que lorsqu'il est testé dans le feu de l'action.

La Phase 3, va permettre de mettre à l'épreuve vos plans, vos stratégies et de vous assurer que chaque membre de l'entreprise est non seulement formé, mais aussi compétent et confiant dans l'exécution de ses responsabilités.

PHASE 3 - VALIDATION

La validation est obligatoire dans le processus de mise en place d'un Plan de Continuité d'Activité opérationnel. Elle représente l'étape d'évaluation rigoureuse de tout ce qui a été élaboré et mis en place de façon théorique. Cette phase vous permet d'effectuer un contrôle approfondi, similaire à un audit de qualité, avant la finalisation complète du PCA.

En testant, surveillant et, finalement, en optimisant votre plan, vous vous assurez de sa robustesse et de sa conformité. C'est la phase de consolidation qui certifie que le PCA est non seulement opérationnel, mais qu'il répond également aux exigences et aux standards définis.

Étape 8 : S'entraîner et tester

La préparation est la clé du succès. Cette étape est consacrée à tester et à s'exercer sur les plans et procédures établis. À travers des tests, des exercices, des simulations, l'entreprise peut identifier les points faibles et renforcer ses stratégies de continuité avant qu'un véritable incident ne se produise.

Tache 25. Définir un programme d'exercices

L'entraînement est un élément essentiel pour assurer la préparation et la réactivité en cas de crise. Il est donc nécessaire de définir un programme d'exercices adapté à l'entreprise.

Ce programme devrait préciser la fréquence, la nature (exercice de table, simulation, bascule réelle) et les scénarios à aborder.

L'objectif est de reproduire des situations qui pourraient potentiellement survenir, afin de permettre aux parties prenantes de s'entraîner régulièrement et d'affiner leurs compétences et réactions.

Tache 26. Déterminer le processus de réalisation des exercices et des tests

Une fois le programme d'exercices défini, il est essentiel de déterminer un processus clair et structuré pour sa mise en œuvre.

Cela inclut la sélection des participants, la préparation du matériel, la définition des objectifs spécifiques de chaque exercice, ainsi que les modalités de suivi et de débriefing.

Ce processus devrait également prévoir des méthodes d'évaluation pour mesurer l'efficacité de l'entraînement.

Suite à ces tests et exercices, il est crucial d'analyser les retours, d'identifier les domaines d'amélioration, et d'ajuster les stratégies et procédures en conséquence.

En testant régulièrement les plans et procédures, vous vous assurez que votre entreprise est de mieux en mieux préparée à répondre efficacement à tout imprévu. Cela permet aussi d'identifier les domaines nécessitant des ajustements ou des améliorations.

10 Clés de la Réussite pour un Exercice de Plan de Continuité d'Activité Efficace

- **Définir les Objectifs :** Avant tout, il est essentiel de définir clairement les objectifs de l'exercice, comme identifier les faiblesses du plan ou tester la réactivité des équipes.
- **Élaborer un Scénario Réaliste :** Le scénario choisi pour l'exercice doit être plausible et pertinent par rapport aux risques identifiés lors de l'analyse de risque.
- **Identifier les Parties Prenantes :** Choisissez avec soin qui participera à l'exercice, incluant non seulement les membres de l'équipe PCA, mais aussi les autres employés et partenaires concernés.
- **Établir un Programme Détaillé :** Élaborez un programme d'exercice clair et détaillé, incluant le timing, les activités à réaliser, et les ressources nécessaires.
- **Prévoir les Ressources Nécessaires :** Assurez-vous que toutes les ressources matérielles, technologiques et humaines nécessaires sont disponibles pour l'exercice.
- **Communiquer Efficacement :** Informez toutes les parties prenantes à l'avance de la date, de l'heure, des objectifs et des attentes de l'exercice, et assurez une communication claire pendant l'exercice.
- **Réaliser une Réunion de Préparation** : Une réunion préalable à l'exercice permet de clarifier les rôles, les responsabilités et les attentes de chacun, et de résoudre les dernières interrogations.
- **Simuler des Conditions Réelles :** L'exercice doit se dérouler dans des conditions aussi proches que possible de la réalité pour évaluer véritablement la préparation et la réactivité de l'organisation.
- **Évaluer et Documenter les Résultats :** Durant l'exercice, observez, évaluez et documentez les performances, les anomalies et les points d'amélioration pour affiner le PCA.
- **Débriefer et Ajuster le PCA :** Après l'exercice, organisez une session de débriefing avec tous les participants pour discuter des retours d'expérience et ajuster le PCA en conséquence.

Étape 9 : Surveiller son PCA

Un PCA n'est pas un document statique déposé sur une étagère poussiéreuse. Il nécessite une surveillance constante pour s'assurer qu'il reste pertinent et efficace face à l'évolution des risques et des besoins de l'entreprise. Cette étape est dédiée à l'évaluation, l'audit et la révision continue du PCA, garantissant son alignement avec les objectifs de l'entreprise.

Tache 27. Auditer son PCA

La surveillance continue du PCA commence par un audit approfondi de ses composants. L'audit permet de vérifier que le PCA est toujours en adéquation avec les besoins actuels de l'entreprise et qu'il est conforme aux normes et réglementations en vigueur. Un audit efficace doit évaluer non seulement la pertinence du plan, mais aussi sa faisabilité, en s'assurant que les ressources nécessaires sont disponibles et que les équipes concernées sont bien formées pour le mettre en œuvre.

Tache 28. Définir des indicateurs de performance

Afin de suivre efficacement la performance et l'efficacité de votre PCA, il est crucial d'établir des indicateurs de performance clairs. Ces indicateurs peuvent inclure le temps nécessaire pour reprendre les activités après une interruption, le niveau de satisfaction des clients pendant une crise, ou encore la capacité à maintenir des niveaux de service prédéfinis. En mesurant régulièrement ces indicateurs, l'entreprise peut rapidement identifier les domaines nécessitant des améliorations et ajuster son PCA en conséquence.

Tache 29. Réaliser des revues de direction

Les revues de direction sont essentielles pour assurer l'alignement du PCA avec les objectifs stratégiques de l'entreprise. Ces revues permettent aux hauts dirigeants d'évaluer l'efficacité du plan, de discuter des retours sur les exercices et tests récents, et de prendre des décisions concernant d'éventuelles mises à jour ou modifications. Ces sessions doivent être l'occasion de réaffirmer l'importance du PCA au sein de l'entreprise, d'allouer les ressources nécessaires à son bon fonctionnement, et de s'assurer que toutes les parties prenantes sont bien informées et impliquées.

La surveillance du PCA est une démarche continue qui vise à garantir que le plan demeure robuste, pertinent et en phase avec les besoins changeants de l'entreprise. Cette étape souligne l'importance d'une approche proactive et de l'engagement continu de la direction pour assurer la résilience organisationnelle.

Quand mettre à jour son PCA?

Cliquer sur l'image

Étape 10 : Améliorer continue de son PCA

Tout comme le monde des affaires est en constante évolution, le PCA doit également évoluer. Cette dernière étape est axée sur la recherche d'opportunités pour renforcer, améliorer et affiner le PCA en fonction des retours d'expérience, des nouvelles menaces et des évolutions technologiques. C'est ici que l'entreprise se prépare pour l'avenir, en s'assurant que son PCA est toujours au meilleur de sa forme.

Tache 30. Traiter les Non-conformités

Afin de garantir l'efficacité optimale du PCA, il est primordial de s'atteler à l'identification et au traitement des non-conformités.

Ces non-conformités peuvent survenir à la suite d'audits, d'exercices, de tests ou encore de véritables incidents. En les identifiant précisément, l'entreprise peut mettre en place des mesures correctives adaptées.

Il convient d'analyser la cause première de chaque non-conformité afin d'éviter sa récurrence.

En outre, ce traitement constitue une occasion pour renforcer les maillons faibles du plan, garantissant ainsi une plus grande robustesse face à des perturbations futures.

Tache 31. Actualiser son PCA

Avec l'évolution des activités, des technologies, des marchés et des menaces, un PCA ne doit pas rester figé.

Il est essentiel de l'actualiser régulièrement pour qu'il demeure pertinent et efficace.

Cette mise à jour peut être dictée par les changements internes à l'entreprise, tels que l'introduction de nouveaux systèmes informatiques, l'expansion vers de nouveaux marchés, ou des changements organisationnels.

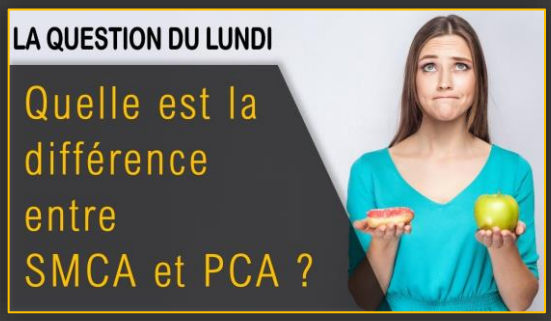
Elle peut également être influencée par des facteurs externes, comme les évolutions réglementaires ou de nouvelles menaces identifiées.

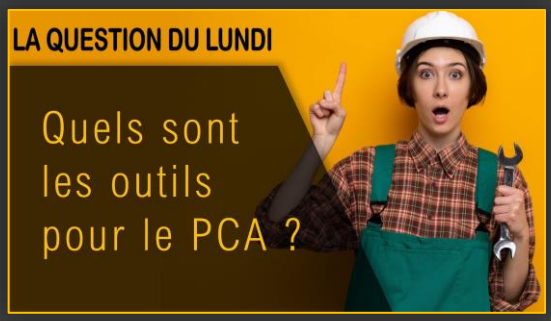
La mise à jour du PCA doit être accompagnée d'une communication claire à toutes les parties prenantes, s'assurant ainsi que chacun est informé des modifications et prêt à agir en conséquence.

Cette étape exige une veille constante et un engagement inébranlable de la part des équipes et de la direction, garantissant ainsi la pérennité et la résilience de l'entreprise face aux imprévus.

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

Compléter vos connaissances avec ces vidéos





Avez-vous lu les autres dossiers du mois ?

Janvier 2023

Avril 2023

Juillet 2023

Le Plan de Continuité d'Activité (PCA) est plus qu'un simple outil de gestion de crise; c'est un pilier stratégique pour toute organisation soucieuse de sa durabilité et de sa réputation sur le marché. Le dossier présenté a minutieusement cartographié les étapes incontournables pour concevoir, déployer et entretenir un PCA robuste, illustrant l'importance d'une approche holistique.

Dès l'amorce, l'analyse des risques et des besoins a jeté les bases de notre démarche. Cette analyse ne s'est pas contentée de dresser un inventaire des menaces, mais elle a permis d'anticiper les enjeux réels pour l'entreprise et de définir les objectifs précis de reprise post-incident. La conception du PCA a ensuite traduit ces objectifs en actions concrètes, en établissant des protocoles et des procédures adaptées à divers scénarios de crise.

Mais un PCA, aussi bien conçu soit-il, reste théorique tant qu'il n'a pas été éprouvé. C'est ici que la validation prend toute son importance.

En simulant des crises, en testant les réactions, l'entreprise se dote d'une véritable expérience, lui permettant d'affiner son PCA, de corriger les lacunes et de renforcer ses points forts. La surveillance et l'amélioration continue du PCA, grâce à des audits, des indicateurs de performance et des revues de direction, garantissent que le PCA reste agile, pertinent et aligné avec l'évolution des enjeux de l'entreprise.

L'importance de la mise en œuvre d'un PCA s'articule autour de plusieurs axes majeurs :

1. Préparation et résilience : Dans un environnement professionnel marqué par l'incertitude, un PCA offre à l'entreprise la capacité de rebondir face aux imprévus, garantissant une reprise d'activité efficiente.

2. Sauvegarde des actifs : Au-delà des actifs matériels, le PCA protège la réputation, le capital humain et les relations d'affaires de l'entreprise.

3. Renforcement de la confiance : Un PCA solide est un gage de sérieux et de professionnalisme, renforçant la confiance des clients, partenaires, actionnaires et employés.

4. Conformité et gouvernance : La mise en place d'un PCA répond souvent à des exigences réglementaires, assurant que l'entreprise respecte les normes de son secteur.

5. Minimisation des conséquences financières : En assurant une reprise rapide, le PCA réduit les coûts liés aux interruptions et préserve la santé financière de l'entreprise.

La mise en œuvre d'un PCA est une démarche stratégique, témoignant de la vision à long terme de l'entreprise. Elle reflète son engagement envers sa mission, ses valeurs, ses clients et ses employés. Dans un monde en constante mutation, posséder un PCA solide est une nécessité pour se démarquer et surtout assurer la continuité et la croissance de ses activités.

Alexandre Fournier et Karine Maréchal

Êtes-vous prêts à affronter une crise ?

Assurez-vous de ne pas être pris au dépourvu !

Pourquoi une formation est cruciale ?

Apprenez à anticiper, gérer et surmonter les interruptions d'activité pour garantir la stabilité et la croissance de votre organisation. Avec des experts du domaine, plongez dans des études de cas réels, des stratégies éprouvées et des outils pratiques.

Outils Pratiques :
Apprenez à créer et appliquer des plans de continuité avec des méthodes et outils éprouvés.

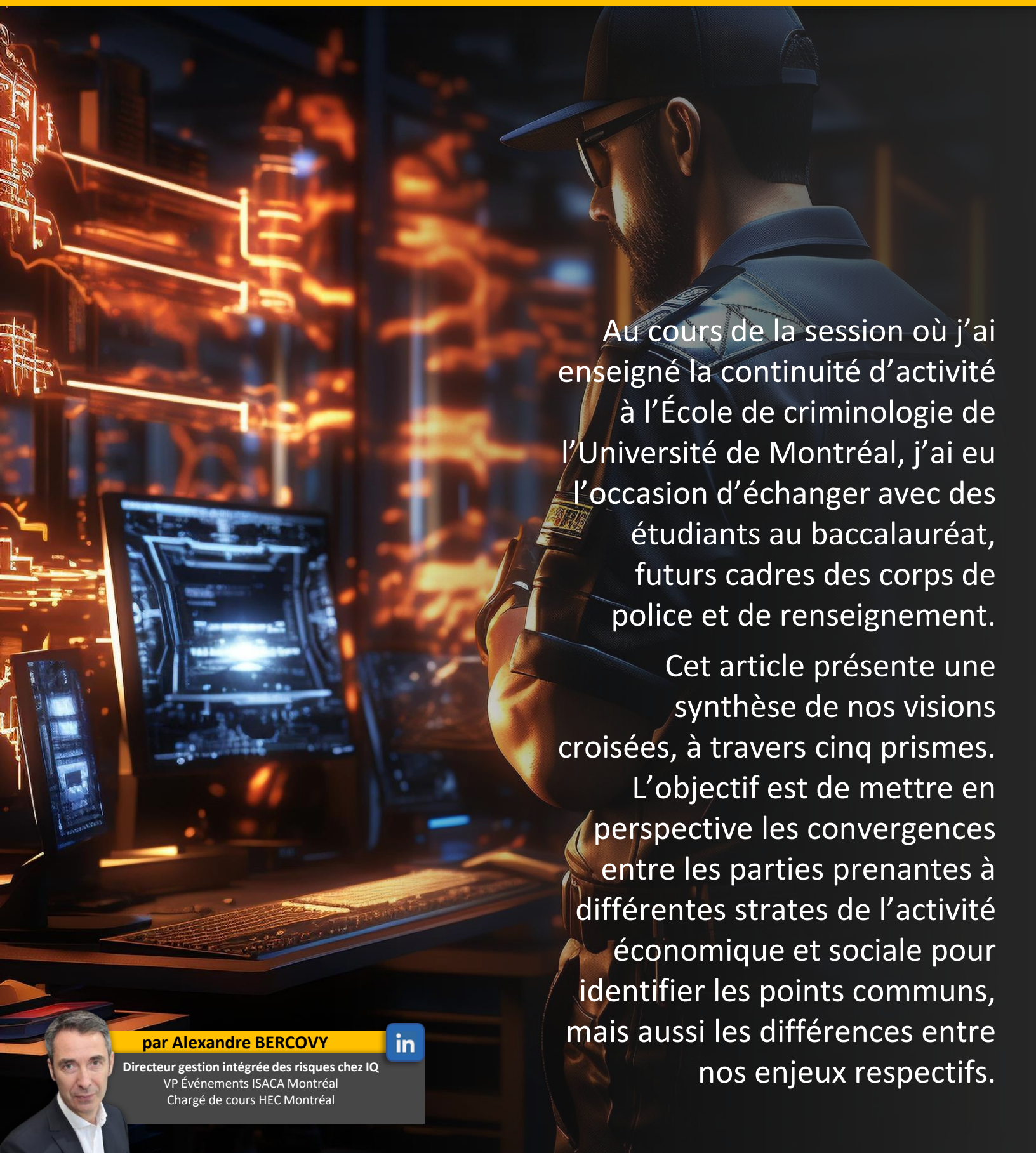
Expertise Professionnelle :
Bénéficiez de l'expérience et des connaissances de formateurs experts dans le domaine.

Réseau Professionnel :
Échangez et apprenez aux côtés d'autres professionnels et leaders du secteur.

Pour en savoir plus cliquez ici

www.crise-resilience.com/formation-pca

La gestion de la continuité vue par le corps policier



Au cours de la session où j'ai enseigné la continuité d'activité à l'École de criminologie de l'Université de Montréal, j'ai eu l'occasion d'échanger avec des étudiants au baccalauréat, futurs cadres des corps de police et de renseignement.

Cet article présente une synthèse de nos visions croisées, à travers cinq prismes. L'objectif est de mettre en perspective les convergences entre les parties prenantes à différentes strates de l'activité économique et sociale pour identifier les points communs, mais aussi les différences entre nos enjeux respectifs.

par Alexandre BERCOVY
Directeur gestion intégrée des risques chez IQ
VP Événements ISACA Montréal
Chargé de cours HEC Montréal

En guise d'introduction, il est important de comprendre la corrélation qui existe entre différents champs de la gestion de risque, à savoir la gestion de la continuité, l'audit, la gestion de crise, les leviers psychologiques utilisés dans le renseignement (Ex : approche MICE) et le triangle de la fraude. Le cas Desjardins, en 2019, a démontré qu'une fraude déclenchée par la dimension M d'un individu pouvait provoquer une crise suivie d'un travail judiciaire impliquant différents corps d'enquête.

Gestion de crise versus prévention

Une confusion commune consiste à confondre la continuité d'activité avec la gestion de crise. Or, il s'agit de deux disciplines distinctes, l'une étant une composante de l'autre. La continuité d'activité englobe l'ensemble des actions à exécuter avant, pendant et après un événement qui perturberait ou interromprait l'activité de l'entreprise. La prévention occupe donc une place prépondérante dans le domaine de la continuité. Sur ce plan, le travail policier est comparable.

Nous voyons agir les policiers, la plupart du temps, dans le cadre d'interventions, mais il faut rappeler que 90 % de leur travail consiste à analyser et à anticiper les crises, dans cette logique de prévention. Ce travail de fond peut prendre plusieurs formes et appellations (conduite du changement, immersion, renseignement…), mais son essence consiste à être au plus près du terrain pendant une longue période, pour détecter les signaux faibles et désamorcer une potentielle perturbation le plus en amont possible.

Pour ce faire, les professionnels s'appuient sur le socle commun de nos disciplines respectives : la gestion des risques. Cette dernière repose sur trois étapes que l'on retrouve dans plusieurs référentiels méthodologiques comme l'ISO 31000, l'ISO 22301, NIST800-53 et la certification CRISC de l'ISACA :

- **Identification des risques :** sur la base de critères tels que la probabilité, l'impact (conséquence), l'intensité, la récurrence, les effets collatéraux, les interdépendances et les mesures de mitigation existantes; cette étape a pour prérequis l'identification des menaces et des vulnérabilités. Quel que soit le cas – une foule pendant un concert, une entreprise située en zone forestière, un réseau informatique – cette phase essentielle nécessite une analyse précise et introspective. Elle produit des scénarios de risques.
- **Analyse des scénarios :** il s'agit ici de déterminer le niveau du risque sur la « cible » que l'on veut protéger en raisonnant spécifiquement sur l'impact. Un même scénario n'aura pas les mêmes conséquences selon l'heure de survenance. Par exemple, une attaque cyber avant le lancement du traitement d'un calcul – octroi de crédit, dispatch d'un staff (affectation d'un personnel) – n'aura pas le même impact qu'après. Il est donc primordial de raisonner sur le cycle entier et non seulement sur un moment précis, soit instant T.
- **Évaluation des risques :** cette évaluation consiste à décider de la stratégie, représentée par le niveau de risque accepté et la limite que l'entreprise ne peut dépasser (capacité).

L'arrivée de personnes chargées d'enquêter est par nature anxiogène, car vécue comme une démarche intrusive.

L'approche MICE en renseignement

L'approche MICE décrit les quatre leviers psychologiques majeurs utilisés en renseignement pour motiver des informateurs :

- **Money** (Argent) : Recrutement via des incitations financières.
- **Ideology** (Idéologie) : Motivation basée sur des convictions personnelles ou politiques.
- **Coercion** (Contrainte) : Utilisation de menaces ou de pressions pour obtenir des informations.
- **Ego** (Égo) : Exploitation du désir de reconnaissance ou de vengeance.

Chaque levier a ses avantages et ses risques, et la clé du succès réside souvent dans la combinaison adaptée à chaque individu.

Audit, analyse, enquête

Le mot « audit » doit être démythifié. Qu'il s'agisse des professionnels du renseignement ou des praticiens de la continuité ou de la vérification, ce mot chapeau recouvre des techniques de collecte d'informations, et son cœur réside dans la vérification basée sur des faits et justifier par des tests. Les policiers sont des professionnels de l'enquête et de l'analyse, ce qui les rend proches des métiers de l'audit et de la gestion de risque. Leurs objectifs sont différents, mais la logique de comprendre l'enchaînement des actions (processus) et de raisonner sur des faits en cherchant à les justifier par des preuves, en prenant en compte le contexte et différentes perspectives, est comparable.

L'arrivée de personnes chargées d'enquêter est par nature anxiogène, car vécue comme une démarche intrusive. Qu'il s'agisse de policiers ou d'auditeurs, les personnes interrogées ressentent la plupart du temps une appréhension et il est primordial de les rassurer en leur rappelant l'objectif du mandat. Ce dernier est de vérifier si un processus donné atteint bien son objectif. Il s'agit de comprendre la situation et non de trouver un coupable.

Dimension procédurale

Les enquêteurs de police interviennent dans la société civile, mais plus rarement en entreprise.

Les processus constituent la colonne vertébrale de l'entreprise. Le travail de continuité et de résilience consiste à inventorier ces processus, à les modéliser et à les trier lors du BIA (Bilan d'Impact sur les Activités). Une méthode pratique et concrète pour réaliser ce travail est d'utiliser des logigrammes qui permettent de représenter les intrants, les extrants, les étapes, les parties prenantes, les risques et les contrôles.

Beaucoup (trop) d'entreprises sous-estiment l'importance de ces documents, par faute de temps ou de moyens. Pourtant, ils sont le point de départ de tout travail de compréhension pour l'analyste en gestion des perturbations et, plus largement, pour toute démarche de transformation.

Entraînement, entraînement, entraînement

La résilience n'est pas un concept qui n'existe que sur papier. La continuité ne peut être efficace que par une pratique fréquente. Ainsi, la conception et la réalisation d'exercices constituent LE nerf de la guerre dans nos disciplines. Trois facteurs clés de succès peuvent être mis de l'avant :

- Les exercices doivent être réalistes et adaptés au contexte –> Est-ce la première fois qu'une simulation est réalisée? Que veut-on tester? Pourquoi? Avec qui? Quel résultat attend-on? Quel est le niveau de maturité des parties impliquées?
- Il est normal de faire des erreurs pendant ces exercices. C'est même leur raison d'être. En entreprise, les personnes engagées doivent comprendre que l'exercice de simulation ne sert pas à les juger ou à les noter sur leur performance. De ce point de vue, les corps policiers et militaires sont beaucoup plus matures et ont pleinement intégré ces exercices dans leur quotidien. Le point ici est de faire deux retours d'expérience, l'un à chaud, l'autre à froid (Ex : méthode GRALE[(1)]).
- Les exercices doivent être pris au sérieux. Les parties prenantes impliquées doivent surtout apprendre et/ou pratiquer la gestion du stress. Qu'il s'agisse d'une prise d'otage ou d'une attaque par rançongiciel, de nombreuses situations ont abouti à un échec parce que les décideurs, même s'ils connaissaient bien l'organisation et les procédures, n'ont pas su faire face au stress lors de situations réelles.

Veille

Qu'il soit question de travail policier ou de continuité d'activité, nous pratiquons des métiers nécessitant une mise à niveau régulière des connaissances et des documents. Dans un environnement en perpétuelle évolution, les solutions et les risques pertinents à l'instant T ne le sont plus quelques mois plus tard *a fortiori* dans un monde à haute vélocité (Internet, changements climatiques, mondialisation). Pour se tenir informé, l'utilisation de sources fiables demeure indispensable. Par exemple, le classement annuel des risques établi par le World Economic Forum (Forum économique mondial) sera utile autant aux policiers qu'aux professionnels du risque et de la continuité.

Conclusion

La continuité d'activité et le travail policier sont *a priori* des disciplines connexes, mais elles convergent pour au moins deux raisons :

- Le travail policier ne se limite pas à la criminalité sociale. La criminalité financière fait pleinement partie de son environnement, de même que la lutte contre la cybercriminalité. Une attaque cyber touchant un réseau de distribution d'eau potable ou de pétrole – comme l'attaque de la compagnie Colonial Pipeline de mai 2021 – peut avoir des conséquences dramatiques. La compréhension des processus et des mécanismes de continuité de l'entreprise est donc une valeur ajoutée pour les équipes qui travaillent sur ces sujets.
- Comme indiqué en introduction, il existe un lien entre la méthodologie de renseignement (Ex : MICE), la gestion de crise et la fraude. La compréhension de ces corrélations est différenciante pour aborder, comprendre et anticiper des crises ou des perturbations.

Le monde de l'entreprise est de plus en plus confronté à un environnement d'incertitudes. Disposer d'outils d'analyse de signaux faibles est un levier, et même un avantage compétitif pour naviguer avec résilience sur un océan d'influences, voire d'ingérences.

Article écrit par Alexandre Bercovy

5 clés pour apporter plus de valeur au mandat

1. Accompagner le changement et expliquer la démarche en tout temps. On n'explique jamais assez!
2. Formaliser les processus de manière graphique. Excel n'est pas un outil de cartographie!
3. S'entraîner : sans exercices de simulation et de debriefing (débreffage), la gestion de la continuité n'a pas de valeur.
4. Effectuer une veille régulière et la mise à jour des documents de soutien.
5. Impliquer dès le départ les parties prenantes de l'écosystème interne et externe.

[(1)] La méthode GRALE

La méthode GRALE guide les retours d'expérience à travers l'analyse factuelle, l'identification de leçons, et leur partage sans jugement préliminaire.

- Gradeless (sans grade)
- Results (Résultat)
- Analyse (Analyse)
- Lessons learned (Leçons apprises)
- Exchange (Echange)

Source : Livre "Au-delà du cockpit" de Pierre-Henri "Até" Chuet, ISBN 979-8410764278.

Alexandre Bercovy CISA, CRISC, CGEIT, CDPSE
Directeur gestion intégrée des risques chez IQ
VP Événements ISACA Montréal
Chargé de cours HEC Montréal

Professionnel chevronné des risques liés aux technologies de l'information, possédant une expérience de 30 ans en sécurité informatique, audit informatique, ERM, projets de transformation. Expert en continuité d'activité et cyber-résilience. Chargé de cours à HEC Montréal et à l'École de criminologie de l'Université de Montréal.

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!

PLUS D'ARTICLES SUR LE SITE DU MAGAZINE

Visitez le site Web du magazine

www.criseetresilience-magazine.com/

La crise, un outil d'influence plus qu'une réalité objective

La terminologie revêt une importance capitale dans la communication et l'expression des idées.

Les mots choisis influencent la perception d'une situation en pouvant lui donner une apparence différente de sa vraie nature, modifiant ainsi son impact émotionnel et donc ses effets.

par Cédric DEBERNARD

Patron de Mutarisk, écrivain, vétéran, humanitaire, atypique modèle multidiplômé

Ancien cadre dirigeant en sûreté internationale

Parmi eux, le mot « crise » est souvent utilisé pour décrire une situation d'urgence, alors que les deux termes recouvrent, dans les faits, des réalités différentes.

Nous vous proposons, dans cet article, d'explorer ce qui les distingue afin d'éviter l'écueil consistant à traiter inutilement n'importe quelle dégradation comme une crise, c'est-à-dire une brutale et incontrôlable situation de rupture, en avançant que la notion de crise relève plus souvent d'une posture de communication que d'une réalité objective.

Avant même de discuter de dégradation, il est primordial de la circonscrire au périmètre auquel celle-ci s'applique, c'est-à-dire le système.

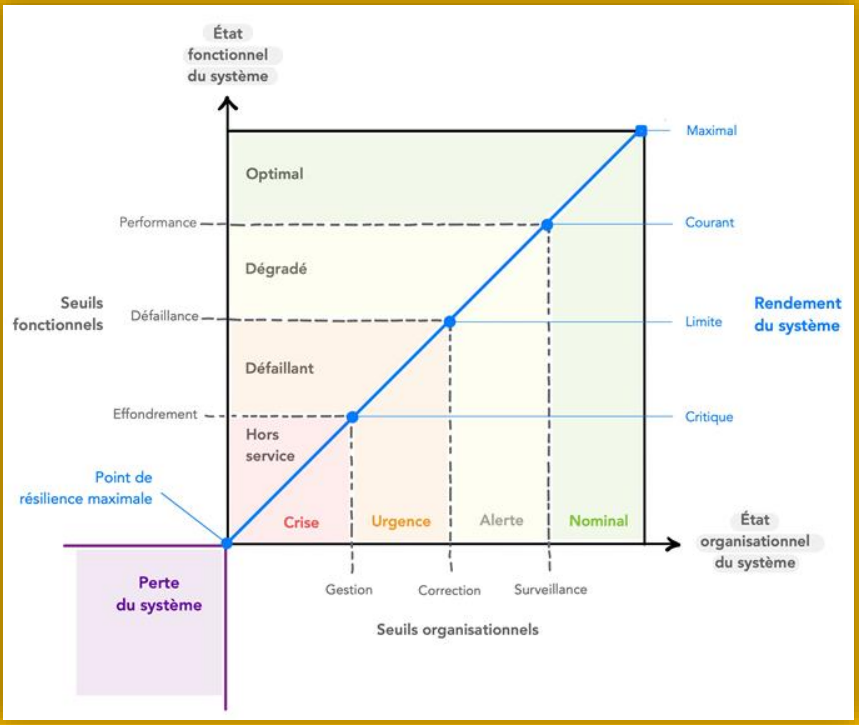
Un système est un ensemble d'éléments en interaction formant un tout, et ayant pour but de réaliser certaines fonctions. Il est en relation avec l'extérieur, qu'il influence et dont il subit l'influence.

Tout système minimalement évolué est composé de sous-systèmes dont l'utilité à la fonction globale est variable.

En 1912, si le Titanic (sous-système) a subi une crise telle qu'il a fini par disparaître, son propriétaire, la White Star Line (système) a réussi à absorber l'impact du naufrage et a continué à fonctionner pendant plus de deux décennies avec d'autres navires (sous-systèmes) tels que le Majestic, l'Olympic ou le Normandie.

Comprendre que la crise de l'un n'est pas la crise de tous, et que la crise d'un composant n'est pas non plus la crise de tout un système permet d'emblée de conserver un sage recul sur les événements.

Graphique illustrant les niveaux de rendement d'un système.



Le rendement d'un système est sa capacité à rendre intégralement le service pour lequel il est prévu. Il se compose d'un état fonctionnel et d'un état organisationnel.

L'état fonctionnel correspond à la restitution effective du service, l'état organisationnel à l'ensemble des mesures permettant au système d'être pleinement fonctionnel. Chacun des deux états peut présenter différents niveaux d'altération ayant pour conséquence une dégradation du service attendu.

Le point de résilience maximale correspond à un seuil au-delà duquel, en plus du service, le système lui-même est perdu. L'impact d'une menace pousse le rendement d'un système vers ce point, tandis que sa capacité de résilience tend à le faire remonter vers son état de rendement maximal.

Idéalement, le rendement du système est maximal (organisation nominale * fonctionnement optimal), mais reste acceptable jusqu'à un seuil courant. Au fil des dégradations, le rendement diminue dans un premier temps jusqu'à un seuil limite (alerte organisationnelle * fonctionnement dégradé) puis un seuil critique (urgence organisationnelle * défaillance fonctionnelle), nécessitant d'être corrigés.

> **" La crise de l'un n'est pas la crise de tous! "**
>
> *Cédric Debernard*

L'urgence correspond donc à une situation où un système ne fournit plus le service prévu, mais répond encore à un certain nombre de mesures déterminées à l'avance visant à le faire revenir à son mode de rendement maximal.

C'est lorsque le rendement d'un système passe en-deçà du seuil critique que l'organisation passe en crise.

Contrairement à l'urgence, la crise se caractérise par un état de décomposition et de déstabilisation profond. Elle représente un bouleversement majeur dans le fonctionnement d'un système, qu'il s'agisse d'une entreprise, d'une organisation ou même d'une société.

La crise survient lorsque les mesures prises pour faire face à une situation d'urgence se révèlent insuffisantes, et que le système est trop en miettes pour que le service attendu ne revienne jamais à l'identique, « comme avant ».

Au sein du système considéré, la crise caractérise donc une rupture par le passage violent d'un avant connu vers un après porteur de changement.

Lors d'une crise, les procédures préétablies et les plans d'action standards ne répondent pas aux besoins de rétablissement du système.

Cette nouvelle et brutale réalité nécessite une réévaluation complète des stratégies, des ressources et des objectifs. Elle exige souvent une prise de décision audacieuse et créative, ainsi qu'une véritable adaptabilité de l'ensemble du système face à l'inconnu.

On admettra aisément qu'elle est relativement rare au sein des organisations.

Alors, si la plupart des situations dégradées ne dépassent pas le stade de l'urgence, pourquoi le terme « crise » est-il si couramment utilisé?

Parce qu'à la différence de l'urgence, la crise est perçue comme un tel état de délabrement qu'elle induit chez l'observateur un vaste éventail de peurs plus ou moins rationnelles.

Peur de l'inconnu, du changement ou de la disparition, crainte pour sa sécurité psychologique ou financière, phobie de la stigmatisation, hantise de la mise en évidence de ses compétences véritables et de sa propre fragilité, incapacité à supporter la perte de contrôle ou l'échec : la gamme est tellement large et la perception tellement personnelle que n'importe quelle situation dégradée ou presque peut être spontanément qualifiée de crise, sans même se poser la question de l'état d'intégrité réel du système et des mesures à disposition pour répondre à sa défaillance.

Requalifier une situation d'urgence en crise légitime des comportements extraordinaires.

D'un côté, le terme permet d'excuser le manque de préparation de l'organisation (« on n'y pouvait rien »), l'incapacité de ses dirigeants à gérer l'urgence (« on a fait ce qu'on a pu »), le sous-investissement en gestion des risques (« on ne pouvait pas prévoir ») ou la prise de mesures d'exception sans justification (« on ne peut pas faire autrement »).

D'un autre côté, faire face à ce qu'on qualifie de crise permet également de débloquer des initiatives, d'ouvrir des postes, d'allouer des budgets.

En cela, le terme « crise » peut objectivement être considéré comme un outil d'influence : il amplifie l'inquiétude, mobilise l'émotion, légitime les actions et oriente la communication institutionnelle.

Son utilisation n'est, la plupart du temps, pas liée à une appréciation objective de la situation, mais au message institutionnel que l'on veut faire passer.

Quelles conséquences pour les gestionnaires de risque?

Plutôt que de se laisser assaillir sans réfléchir par la crainte du pire, mieux vaut démystifier la dégradation observée en la ramenant à sa capacité de nuisance pour le système considéré. Si la situation est maîtrisée grâce à l'application de procédures et de processus déterminés à l'avance, il s'agit au pire d'une situation d'urgence qui ne remettra pas en cause la survie du système.

On obtient alors une analyse rassurante à livrer aux décideurs, qui s'attendront à un prochain retour à la normale.

À l'opposé, on peut délibérément choisir d'utiliser le terme « crise » dans deux circonstances :

- d'une part, lorsque le système, ayant dépassé le seuil d'effondrement, est véritablement en crise;
- d'autre part, lorsque l'on veut lancer un avertissement sans équivoque sur certains manques organisationnels ou fonctionnels en gestion des risques.

Désormais, lorsque vous entendrez le terme « crise », détendez-vous, car il est très probable que ce n'en soit pas une.

Et si par hasard celle-ci venait à frapper, renoncez d'emblée à l'idée d'une « gestion de crise » illusoire pour vous concentrer sur l'imagination et la capacité à innover en vue d'un futur différent.

Un futur où le service prévu, voire le système censé le produire, auront définitivement disparu

Article écrit par Cédric Debernard

Cédric Debernard est aux commandes de Mutarisk. Ancien cadre dirigeant en sûreté, il aligne une vaste expérience internationale acquise dans plus de trente pays sur cinq continents dans les secteurs de l'énergie, l'ingénierie et construction, la consultation, les ONG, la défense nationale et la police.

Il poursuit également une activité d'auteur. Oscillant subtilement entre fiction et réalité, son écriture s'appuie sur une carrière riche de fabuleuses expériences et de rencontres privilégiées dont il s'inspire largement. Son premier roman, Furor Arma, a été publié en septembre 2020 aux Éditions La Plume d'Or (Québec).

Suivez Cédric, sur mutarisk.com et cedricdebernard.com


“
Un incident est une petite pierre sur votre chemin.
Une crise, c'est quand cette pierre se transforme en boule de démolition.
”

La crise cyber à 360°, sinon rien…

En 2017, en tant que négociateur au GIGN, je gère le premier ransomware (rançongiciel) pris en charge par la Gendarmerie et je vais découvrir la « tarte Tatin » de la cybercrise.

Je mets le doigt dans un engrenage qui va, contre l'avis de ma hiérarchie de l'époque, me pousser à gérer la crise de manière systémique en outrepassant mes prérogatives de départ…

par David CORONA

Gestion de crise cyber et négociation

Ex-négociateur du Groupe d'intervention de la Gendarmerie nationale (GIGN) et cofondateur de l'agence In-Cognita, spécialisée en gestion de crise cyber et en négociations à fort enjeu.

Dans le récit qui va suivre, toute ressemblance avec des organisations, des personnes ou des faits réels serait absolument fortuite… ☺

Bordel organisé

Il est 7 h 30 du matin, un samedi, et l'incident informatique qui bloque la production et la prise de rendez-vous de cette entreprise est technique. Il touche toutes les branches de la société et, par extension, ses clients et fournisseurs.

Les dirigeants sont dans le brouillard, ils posent des questions auxquelles ils n'auront pas, dans l'immédiat, de réponses. Ce qui est censé ressembler à une cellule de crise est plus proche d'une scène de ménage professionnelle.

Les émotions sont aux commandes; c'est normal dans ces moments-là, et nous ne sommes qu'à la quinzième minute après que le responsable informatique eut exposé l'ampleur des dégâts.

Un dirigeant demande au responsable commercial de se préparer à contacter les clients et les fournisseurs, et au directeur des opérations de mettre en œuvre les plans de continuité des activités (PCA).

Seul hic, toutes ces informations sont sur les ordinateurs, qui sont eux-mêmes inaccessibles…

Qu'à cela ne tienne, l'assureur arrive et pose une somme importante pour couvrir les pertes et, surtout, pour payer la rançon de 1 million d'euros en Bitcoin demandée par les pirates informatique. Les actionnaires demandent au PDG de régler le problème rapidement. Ce dernier se tourne vers son directeur de la sécurité de l'information, lequel doit faire face à une myriade d'acteurs techniques qui ont autant de questions que de réponses et qui ne sont pas en mesure de donner un délai de redémarrage des opérations naturellement.

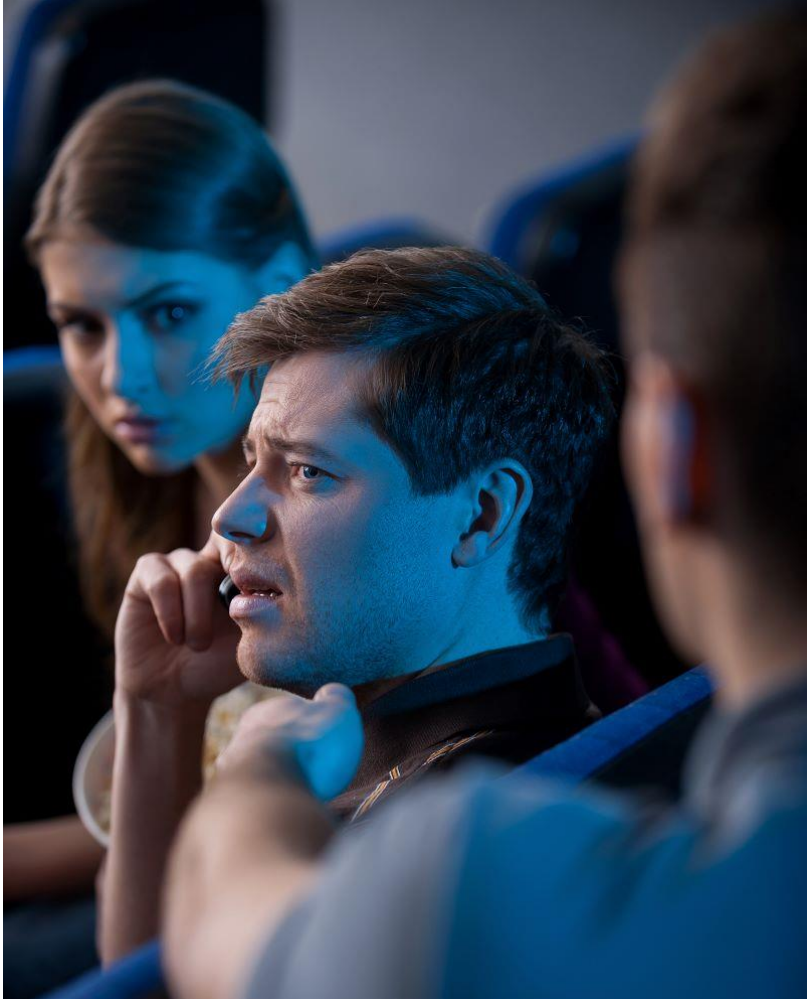
Là-dessus, la responsable du service des communications demande ce qu'il faut dire précisément en interne et en externe, car ça commence à parler dans les unités de production, et deux journalistes ayant eu vent d'une cyberattaque ont appelé le standard du siège.

Le responsable du service juridique le met en garde au sujet du discours à produire, car, dit-il, nous sommes tenus par des contrats qui font en sorte que notre responsabilité pourrait être engagée en ce qui concerne notre gestion de l'incident.

La tension est à son comble…

Toute la souplesse de l'organisation se cristallise au fil des minutes et des mauvaises nouvelles…

> **“ La crise « technique » ne trouvera d'issue favorable que par une bonne gestion humaine. ”**
>
> *David Corona*



Mais voyons plutôt ce qui aurait pu être mis en place en amont pour éviter d'en arriver à un point où la résilience d'une organisation se rapproche de 0.

Charité bien ordonnée commence par soi-même

Se préparer pour faire face à une crise cyber se limite souvent à donner du budget à son responsable des technologies de l'information (TI), à donner une formation de deux jours par an au comité de direction (CODIR) et à charger la personne responsable de la responsabilité sociétale de l'entreprise (RSE) (environnement, bien-être au travail, etc.) de mettre en place des PCA.

Être réellement prêt est une autre paire de manches… Pour cela, il faut avoir :

- Une doctrine et un plan de gestion de crise uniformes dans l'organisation;
- Un organigramme de cellule de crise et un processus de déclenchement de cette dernière;
- Une chaîne d'alerte et des personnes d'astreinte bien convenues;
- Les documents essentiels (PCA, liste clients/fournisseurs) déconnectés du réseau et accessibles;
- Des canaux de communication clairs et prêts à l'usage en cas de crise cyber (téléphonie, visioconférence);
- Une expérience pertinente, soit avoir vécu au moins une fois par an un exercice majeur de gestion de crise cyber.

Les 4 piliers

Pour aller plus loin et en même temps se rapprocher de l'essence de la gestion d'une crise cyber, il faudrait structurer son organisation de crise selon les piliers suivants :

- Pôle Décisions (gère la stratégie et les conséquences des actions pour piloter la crise);
- Pôle Opérations (constitue le bras armé des décisionnaires sur le terrain);
- Pôle Coordination (gère les interactions au sein et en dehors de la cellule de crise, organise les points de situation et la logistique);
- Pôle Chronologie (représente la main courante de la crise et servira pour le retour d'expérience et/ou l'exploitation judiciaire des actions et des prises de décision).

Un poste pour chacun et chacun à son poste. Une cellule de crise se déclenche en comité restreint et s'étoffe au fur et à mesure des événements afin d'éviter la cacophonie de départ.

On peut donc y ajouter par la suite et dans un temps court les responsables des communications, des finances, des ressources humaines, de la sûreté/sécurité, juridiques…

Le cas échéant, il est judicieux de se faire accompagner de manière périphérique par des spécialistes de la gestion émotionnelle et psychologique ainsi que par un(e) négociateur(-trice) au besoin.

Mais, dans tous les cas, lors du premier tour de table et jusqu'au dernier, le dirigeant devra parler en dernier afin de ne pas inhiber les collaborateurs, de pouvoir bénéficier de leur libre parole et ainsi d'avoir un maximum d'éléments pour prendre ce qu'il estime être la bonne décision.

Les 5 conseils de la crise cyber

1. Respirez avant de vous jeter dans l'action, vous allez avoir besoin de tous vos neurones et d'un recul suffisant pour vous engager correctement dans la crise.
2. Ne répondez pas aux hackers (pirates informatiques) en cas de demande de rançon. Vous le ferez éventuellement quand vos équipes seront réunies et prêtes à agir.
3. Mettez en place une structure de gestion de crise au sein de votre organisation (doctrine, chaîne d'alerte, coordination, décisions, chronologie, documents essentiels déconnectés du réseau et accessibles).
4. Agissez aussi vite que possible et aussi lentement que nécessaire. L'émotion n'est pas un bon pilote dans la crise.
5. Entraînez-vous en équipe aussi souvent que possible lors de cas fictifs inspirés du réel et tirez-en des enseignements qui doivent si possible se transformer en actions correctrices.

Conclusion

Il y a une réelle différence entre se préparer et être prêt. Malheureusement, on l'apprend souvent à ses dépens lors d'un incident réel. N'attendez pas d'avoir des moyens considérables ou de pouvoir organiser un exercice majeur avant de commencer à structurer votre gestion de crise.

Les bons réflexes et les bonnes pratiques peuvent se mettre en place de manière simple, à petite échelle au départ pour les tester. Ils pourront ensuite être dupliqués au sein de l'organisation tout entière.

Nul besoin d'être une grande entreprise pour avoir un plan de gestion de crise, car c'est l'adaptabilité de la structure qui assurera sa survie en cas d'incident majeur… quelle que soit sa taille.

Il y a trois façons de traverser une crise : s'éteindre, s'abîmer, s'améliorer.

Choisissez votre camp!

David Corona Gestion de crise et négociation

Ex-négociateur du Groupe d'intervention de la Gendarmerie nationale (GIGN) et cofondateur de l'agence In-Cognita, spécialisée en gestion de crise cyber et en négociations à fort enjeu.

Le paysage numérique est rempli de menaces imprévues.

Apprenez les étapes essentielles pour gérer une Crise de type « Cyberattaque ».

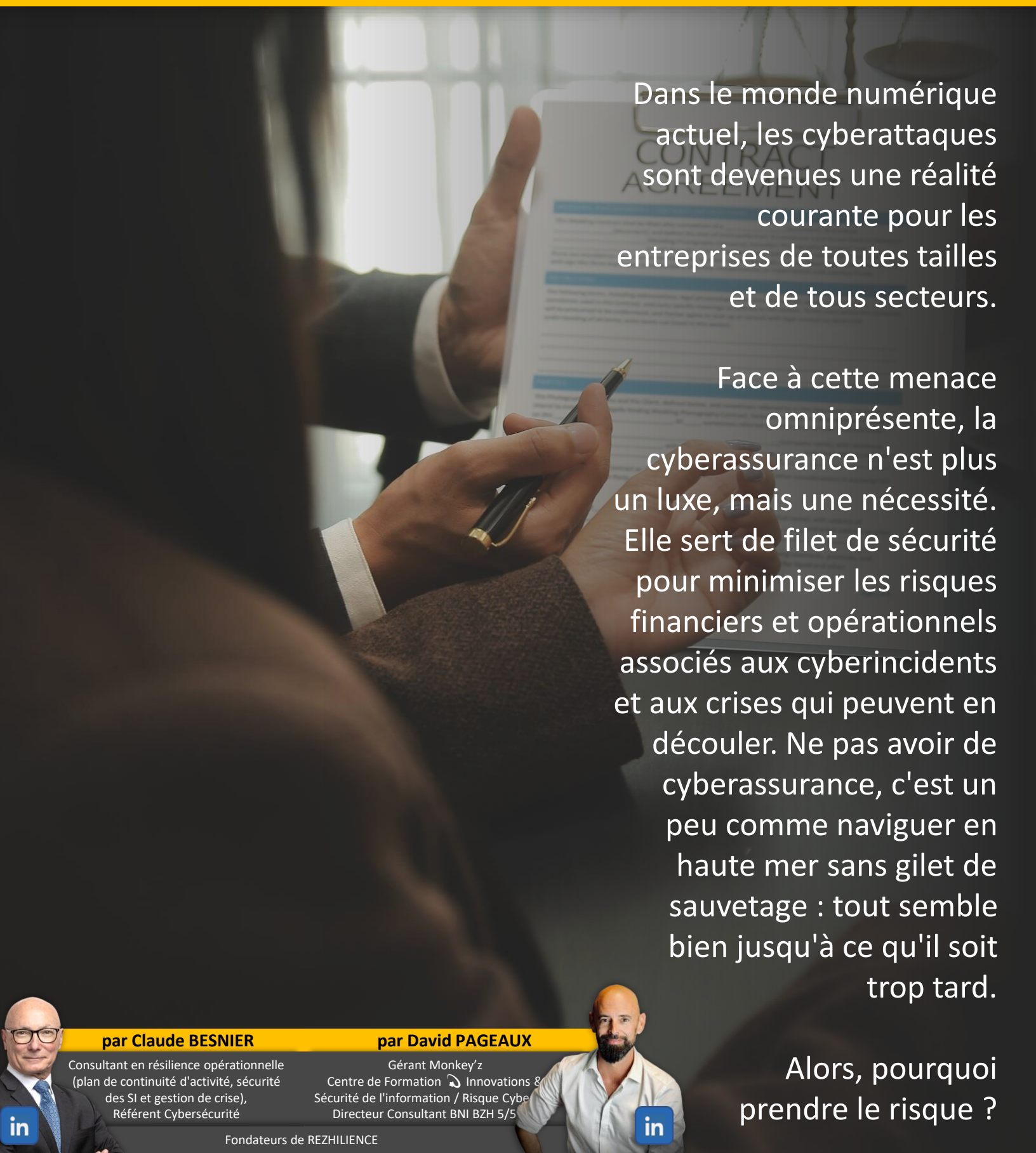
Renforcez vos compétences et assurez la survie de votre entreprise.

Prochaine formation

En savoir plus

www.crise-resilience.com/cybercrise

Assurance Cyber
les éléments clés de la résilience



Dans le monde numérique actuel, les cyberattaques sont devenues une réalité courante pour les entreprises de toutes tailles et de tous secteurs.

Face à cette menace omniprésente, la cyberassurance n'est plus un luxe, mais une nécessité. Elle sert de filet de sécurité pour minimiser les risques financiers et opérationnels associés aux cyberincidents et aux crises qui peuvent en découler. Ne pas avoir de cyberassurance, c'est un peu comme naviguer en haute mer sans gilet de sauvetage : tout semble bien jusqu'à ce qu'il soit trop tard.

Alors, pourquoi prendre le risque ?

par Claude BESNIER

Consultant en résilience opérationnelle (plan de continuité d'activité, sécurité des SI et gestion de crise), Référent Cybersécurité

par David PAGEAUX

Gérant Monkey'z
Centre de Formation Innovations &
Sécurité de l'information / Risque Cybe
Directeur Consultant BNI BZH 5/5

Fondateurs de REZHILIENCE

I. Qu'est-ce que l'assurance cyber?

L'assurance cyber est un contrat qui offre une protection financière contre les pertes causées par des cyberattaques et les violations de données.

Cette assurance aide les entreprises à couvrir les coûts liés à la remédiation des violations de données, à la restauration des systèmes et des données, à la notification des parties prenantes concernées et aux poursuites éventuelles.

L'assurance cyber va apporter une assistance en matière de gestion de crise, y compris en matière de communication avec les parties prenantes, d'analyse forensique (investigation numérique) et de récupération des données.

Le contrat peut également prévoir la prise en charge des frais relatifs au maintien ou à la restauration de la réputation de l'entreprise.

En souscrivant une assurance cyber, les entreprises peuvent se protéger contre les coûts de gestion de crise et de relations publiques qui peuvent survenir à la suite d'une telle violation.

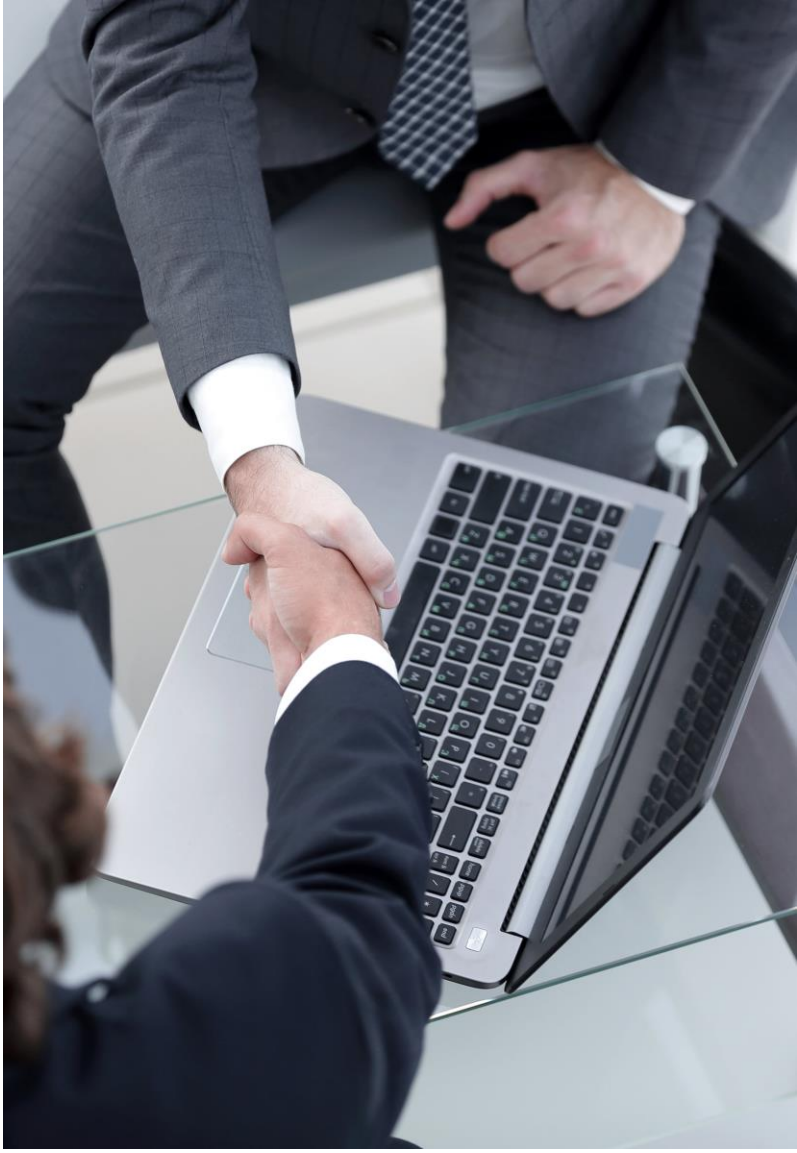
Il est important de noter que toutes les polices d'assurance cyber ne sont pas identiques.

Les entreprises doivent examiner attentivement les termes et les conditions de chaque police, en particulier en ce qui concerne les exclusions et les plafonds de couverture.

Cette relation contractuelle liée à la sécurisation de l'entreprise doit s'inscrire dans la confiance, et il est essentiel que les entreprises travaillent en étroite collaboration avec leurs assureurs pour s'assurer qu'elles ont une couverture adéquate en fonction de leurs risques et de leurs besoins (mais cette démarche n'est pas exclusive au risque cyber…).

" Le coût moyen d'une attaque de logiciels malveillants contre une entreprise est de 2,4 millions de dollars. "

Accenture



II. Les avantages de l'assurance cyber pour la résilience de l'entreprise

Au-delà de la couverture des pertes financières résultant d'une cyberattaque ou d'une violation de données et de l'assistance contractuelle spécialisée (comme indiqué ci-dessus), intégrer un assureur dans la démarche de sécurisation de son entreprise face au risque cyber revêt des avantages supplémentaires essentiels.

En effet, en souscrivant une police d'assurance cyber, les entreprises doivent généralement suivre certaines pratiques de sécurité informatique pour être admissibles à la couverture.

Cela peut inclure la mise en place de mesures de sécurité de base, telles que l'utilisation de mots de passe forts et l'installation de logiciels antivirus.

En suivant ces pratiques, les entreprises peuvent réduire leur risque de subir une violation de données ou une cyberattaque.

Cet examen des pratiques de sécurité informatique peut également aider les entreprises à prendre conscience de leur vulnérabilité aux cyberattaques et à mieux comprendre les mesures qu'elles peuvent prendre pour se protéger.

Cela peut aider à renforcer la culture de la sécurité informatique au sein de l'entreprise et à améliorer la sensibilisation des employés aux menaces de sécurité.

III. Les éléments clés de la résilience en matière d'assurance cyber

Lorsqu'il s'agit de la résilience en matière d'assurance cyber, il y a plusieurs éléments clés à considérer pour aider les entreprises à se protéger contre les cyberattaques et les violations de données.

Pour souscrire une assurance dans les meilleures conditions, il faut satisfaire à plusieurs points :

- **Évaluer les risques :** il s'agit d'identifier les menaces potentielles et les vulnérabilités associées à l'architecture du système d'information, aux politiques d'habilitation, à la mise à jour des versions logicielles, aux antivirus, etc.
- **Identifier les données sensibles et les systèmes critiques :** une cartographie précise des données et des systèmes critiques permet de concentrer les efforts de sécurité là où ils sont nécessaires.
- **Mettre en place un dispositif de gestion de crise :** avoir un plan d'action clair pour répondre rapidement et efficacement aux cyberattaques est crucial pour minimiser les dommages potentiels.
- **Élaborer un plan d'action avec des mesures préventives et curatives :** des mesures préventives robustes doivent être mises en place pour réduire le risque de cyberattaque, tandis que des mesures curatives permettront de réagir rapidement en cas d'incident.
- **Surveiller en permanence l'environnement informatique et évaluer régulièrement le programme de sécurité informatique :** la cybersécurité est un processus continu, et les entreprises doivent surveiller et évaluer régulièrement leur posture en matière de sécurité pour s'assurer qu'elle reste efficace face aux menaces en constante évolution.

  Cela peut inclure l'utilisation d'outils de surveillance de la sécurité, la conduite régulière de tests de pénétration et l'analyse des incidents de sécurité passés pour identifier les possibilités d'amélioration.
- **Sensibiliser et former les employés à la sécurité informatique :** la sensibilisation et la formation des employés sont essentielles pour renforcer la culture de la sécurité au sein de l'entreprise et réduire les risques liés aux erreurs humaines.

L'assurance cyber peut ainsi offrir plusieurs avantages pour renforcer la résilience de l'entreprise face aux cybermenaces.

Elle peut offrir une assistance en cas d'incident, réduire le risque de subir une violation de données ou une cyberattaque, sensibiliser à la sécurité, offrir une réponse plus rapide en cas d'incident et protéger la réputation de l'entreprise.

7 clés pour améliorer la résilience en matière de cybersécurité :

- Évaluer les risques et les menaces;
- Élaborer et mettre en place un plan de gestion de crise;
- Mettre en place des mesures de sécurité robustes;
- Former les employés à la sécurité informatique;
- Établir des relations de confiance avec les partenaires et les fournisseurs;
- Évaluer et tester régulièrement l'efficacité des mesures de sécurité (permet aussi de couvrir le risque résiduel);
- Souscrire une assurance cyber adaptée à ses enjeux, à son environnement et au risque résiduel après mise en application des points précédents.

En combinant ces avantages avec les éléments clés de la résilience en matière d'assurance cyber, les entreprises peuvent renforcer leur posture en sécurité informatique et se protéger.

En somme, l'assurance cyber doit être une partie importante de la stratégie globale de résilience d'une entreprise, mais elle ne peut être considérée comme la seule et unique solution face au risque cyber. L'assureur est l'un des maillons de la chaîne de protection contre ce risque.

La mise en place de mesures de sécurité solides, la sensibilisation des employés à la sécurité informatique et la planification de la gestion de crise sont également des éléments clés pour renforcer la résilience de l'entreprise.

L'utilisation d'une matrice de maturité telle que celle que nous pouvons proposer permet aux entreprises de prendre des mesures afin de se protéger contre les cyberattaques et ainsi de maintenir une culture de la sécurité.

Article écrit par David Pageaux et Claude Besnier

David Pageaux, a créé **MKZ Assurances**, cabinet de courtage en assurances spécialisé en risque cyber, et **Monkey'Z**, société de conseil et centre de formation consacré à la sécurité de l'information, aux innovations technologiques et à la gestion de crise.
Claude Besnier, est expert en résilience opérationnelle et en gestion de crise et référent en cybersécurité auprès des PME.

En 2022, ils ont fondé **REZHILIENCE** dans l'objectif de réunir des professionnels et des experts et de travailler ensemble afin d'apporter une solution globale de sécurisation de l'environnement numérique, en analysant les risques et en mettant en place des mesures de gestion de crise adaptées.

REZHILIENCE, est une société spécialisée dans la résilience opérationnelle, la gestion des risques liés à la cybersécurité et la gestion de crise.

Nous travaillons à mettre en évidence les éléments clés de la résilience en matière de risque cyber pour aider les entreprises à se protéger contre les cyberattaques et les violations de données.

En savoir plus : https://www.rezhilience.fr/

Deviens un acteur de la cybersécurité de ton entreprise

Si ta grand-mère est capable de trouver ton mot de passe…

CHANGE-LE VITE!

Affiche de sensibilisation offerte par Crise et Résilience – www.crise-resilience.com

CRISE & RÉSILIENCE

Contrôler son émotion : attention à la surcrise

Pour moi qui suis issue du monde de la thérapie, il est toujours assez saisissant d'arriver en entreprise pour intervenir sur une gestion de crise ou pour proposer un exercice et de me rendre compte qu'il s'y véhicule encore parfois des idées aussi dépassées que tenaces sur les émotions et sur la façon dont nous devrions les gérer, ou plutôt les « contrôler », lorsqu'une situation tendue se présente.

par Anne-Gervaise VENDANGE

Experte en profilage, en influence, en gestion et en communication de crise.

Co-fondatrice de In-Cognita

Et par « contrôler », entendez « arriver à l'instar d'un robot à ne rien ressentir pour agir avec froideur ». Étonnant. Comme si cela était devenu, à un moment de l'évolution de nos croyances sur notre condition humaine, un gage d'efficacité. Nos chers stoïciens, si leur travail est incommensurable en termes d'apport à l'humanité, n'y sont sûrement pas pour rien, bien aidés par quelques héros mythologiques et certains bons blockbusters (superproductions) hollywoodiens.

Or, le principe même d'une émotion est que nous n'avons pas de prise dessus. Elle vient ou ne vient pas, reste acceptable ou déborde, mais en aucun cas vous n'en avez la télécommande. C'est là tout l'objet du travail de l'école de Palo Alto sur les notions de processif et de réflexif. Tenter de contrôler les processus automatisés de notre corps (pulsions, émotions, envies…) avec notre tête amènera à les radicaliser. C'est le cas par exemple de la procrastination ou de l'insomnie : ce n'est pas votre tête qui décide enfin de s'endormir, mais votre corps, et si vous réfléchissez à comment faire, vous ne dormez pas.

Par ailleurs, « gérer » en évitant est un non-sens. Imaginons que nous partions en mer et que je vous demande de gérer le bateau. Si vous en descendez, vous n'aurez rien géré du tout. C'est à peu près aussi absurde que de gérer une émotion en lui demandant de ne plus être là.

L'émotion dans la crise, une colocataire parfois gênante.

Le mot « émotion » vient du latin emovere, qui signifie « mettre en mouvement ». Ce mécanisme du corps permet d'être adapté à une situation et de combler un besoin. Ainsi, quoi de plus logique, face à une crise et donc à un danger potentiel, que votre corps cherche à vous mettre en mouvement, à vous rendre adapté à l'enjeu?

La peur et ses dérivés, comme le stress, ont avant tout la vocation d'assurer votre mise en sécurité.

La colère, et son énergie très exocentrée, vous permet de créer du changement;

et la joie, parfois si explosive, raconte votre besoin de partage.

En somme, une émotion est un messager, un peu comme un postier qui viendrait nous livrer un courrier recommandé.

C'est souvent peu agréable, mais en vouloir au postier n'aurait aucun sens.

C'est le message contenu dans cette lettre qui peut éventuellement vous contrarier. Le postier, lui, n'y est pour rien : il veut simplement faire son travail.

Alors, convenons-en, celui-ci est un peu acharné. Sans réponse, il se présentera encore et encore, sous des formes diverses et de plus en plus pressantes, jusqu'à parfois enfoncer votre porte pour être entendu – comprenez : « vous surprendra avec une émotion incontrôlable ».

Paradoxalement, c'est cette peur de perdre le contrôle qui nous empêche souvent d'ouvrir notre porte et qui finit irrémédiablement par générer le high kick (coup de pied) bien senti qu'il mettra dedans.

Problème : lorsque l'on ressent fortement une émotion, il est souvent compliqué d'avoir concomitamment une réflexion pertinente.

Or, en gestion de crise, nous avons besoin de toute notre capacité tactique et stratégique, c'est vrai.

Mais, vous l'aurez maintenant compris, en rejetant cette émotion, nous prenons aussi le risque d'avoir un répit de celle-ci, tout en ne maîtrisant pas le moment où elle se représentera, ou de la renforcer et qu'elle devienne incontrôlable.

Mais revenons-en à notre contexte. Une crise est, par essence, un événement à fort potentiel de déstabilisation pour l'organisation. Les corps ont donc tout un tas de messages à nous livrer et, bien naturellement, des émotions se déclenchent. Rien d'étonnant, donc, à ce que la peur et la colère se montrent régulièrement en premier lieu. Contournons ici un instant l'émotion pour regarder le besoin qu'elle exprime. Si vous arrivez à ce que la situation change (colère) afin de vous mettre en sécurité (peur), alors la crise s'arrêtera. Ce que vous propose votre corps paraît donc plutôt censé.

Prenons l'exemple de la crise cyber.

La séquence émotionnelle commence souvent par la colère plus ou moins contenue d'un dirigeant qui demande à son directeur de la sécurité de l'information (DSI) de combien de temps il a besoin pour, au choix, avoir une idée de ce qui passe et de l'étendue de ce qui est touché et/ou recouvrer une fonctionnalité normale.

Le DSI répond qu'il ne sait pas. C'est vrai, il n'en a aucune fichue idée. Son supérieur commence à percevoir qu'il ne va pas être aussi facile de reprendre le contrôle…

Eh oui, les premiers instants d'une crise cyber nous laissent toujours un peu démunis. Les trente premières minutes sont rarement bonnes conseillères, et attendre de laisser l'émotion faire son travail devrait permettre de rapidement vous laisser accès à votre capacité stratégique. Avant de peut-être pouvoir, dans quelques heures ou quelques jours, exprimer votre joie et votre soulagement.

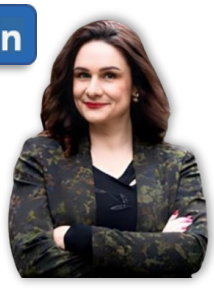
Et, pour finir, soyez bienveillant aussi avec les émotions des autres. Une crise est un moment particulier qui met les individus à rude épreuve. Dans la limite de votre intégrité, ne tenez pas rigueur aux autres de leur émotion dans la tempête. Être capables de passer par ces moments houleux ensemble vous renforcera en tant qu'équipe et vous fera gagner une expérience aussi stratégique qu'émotionnelle pour les enjeux à venir.

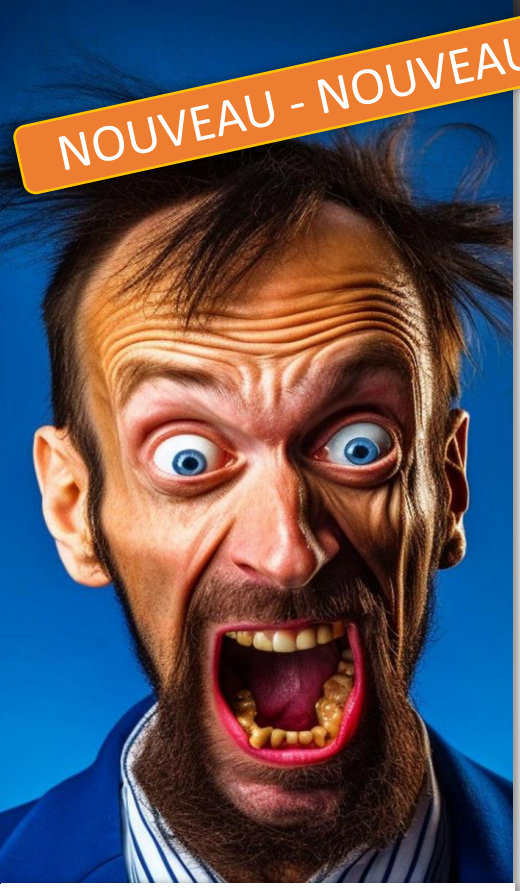
Et concrètement?

- **Entraînez-vous régulièrement.** Plus de d'habitude = moins d'émotion. C'est ainsi que vous gérez sans doute calmement aujourd'hui des choses qui vous ont stressé dans le passé.
- **Ne combattez pas votre émotion, collaborez avec elle.** Reconnaissez votre besoin, normalisez-le. Une émotion ne se juge pas, sa simple présence la justifie. Vous êtes un être humain et c'est une bonne nouvelle, car c'est exactement ce dont nous avons besoin pour nous sortir de là!
- **Imaginez le pire de ce qui pourrait se passer**. C'est assez contre-intuitif, mais efficace. Évidemment, c'est intéressant en termes de prise de décision, mais cela va aussi dire à votre émotion que vous êtes conscient de l'enjeu. Éviter d'y penser lui enverrait le message inverse et la rendrait plus puissante. Ainsi, vous devriez sentir votre émotion se calmer rapidement.
- **Il est possible de donner rendez-vous à son émotion.** Si vous sentez qu'elle déborde, dites-lui que vous l'avez entendue, mais que vous n'êtes pas disponible maintenant. Lorsque vous serez seul, prenez sincèrement un temps pour la ressentir. C'est ainsi que l'on peut passer le trajet de retour du travail à rejouer la joute verbale du midi avec Joséphine de la comptabilité. Ce mécanisme est salvateur si et seulement si vous ne lui demandez pas de se mettre à l'écart pour ne jamais l'accueillir; elle saurait s'en souvenir.

Anne-Gervaise Vendange
Experte en profilage, en influence, en gestion et en communication de crise.

Après avoir accompagné des milliers de personnes en crise personnelle, elle crée en 2021 In-Cognita, pour déployer son savoir-faire à plus grande échelle.





5 conseils anti-stress

simples et sans contraintes.

La santé est notre bien le plus précieux, particulièrement lors de situations de crise. Elle nous donne la force nécessaire pour résister à la pression, pour prendre des décisions éclairées et pour, finalement, en ressortir indemne et en pleine forme.

C'est dans cette optique que nous avons décidé d'introduire une rubrique dédiée à la relaxation dans chaque numéro de notre magazine. Nous espérons qu'elle vous offrira des informations et des conseils précieux pour maintenir et renforcer votre bien-être, même dans les moments les plus éprouvants.

Timothy Mirthil-de Segonzac

Journaliste et auteur spécialiste de la gestion du stress

Auteur du livre « Les 5 temples »
(cerveau, cœur, ventre, sexe, respiration) - Écologie corporelle pour réveiller votre puissance intérieure : exercices de respiration, méditation, bains froids, apnée, visualisation

Si j'avais la chance de remonter le temps et de rencontrer mon moi d'il y a 20 ans, voici les 5 conseils anti-stress simples et sans contraintes que je me donnerais :

La respiration Matrix

- inspire 4 secondes,
- retiens ton souffle 4 secondes,
- expire 4 secondes,
- retiens 4 secondes.

En à peine 4 minutes, c'est incroyable comme cette technique peut apaiser l'esprit et en même temps améliorer le focus puis le passage à l'action.

Le magnésium magique

Ce minéral magique, joue un rôle crucial dans notre réponse au stress. En période de tension, notre corps a tendance à épuiser ses réserves de magnésium. Il est donc essentiel de maintenir un niveau adéquat de magnésium pour aider à réguler notre système nerveux, favoriser la détente musculaire et améliorer la qualité de notre sommeil.

La force de la marche

La marche est un puisant remède anti-stress. Elle permet de prendre du recul, de se déconnecter tout en libérant des endorphines qui boostent le moral. Quand tu te sens submergé, passe à l'action.

Le sommeil, ton allié

Un sommeil régulier et de qualité est la base d'une vie sans stress. La récupération est l'angle mort de la vie moderne. Alors quand la fatigue est trop présente, respecte un peu plus ton rythme circadien. Même heure de coucher, même heure de réveil pendant un mois et tu recharges tes batteries au max.

La confiance en toi

La confiance en soi est le rempart ultime contre le stress. Crois en tes compétences et en ton aptitude à surmonter les défis. Fais confiance aux autres.

Celui-ci... c'est cadeau 😄

Et prend des murs de temps à autres, ça renforcera ta capacité à devoir choisir les bons chemins.

Voilà 5 conseils sans contraintes jeune homme.

Passe à l'action!

Avec le DORA, explorez la résilience de votre entité financière

Le règlement européen **Digital Operational Resilience Act (DORA)** encadre la réponse du secteur financier face aux risques et aux menaces numériques.

Cette approche globale fonde la stratégie de résilience et donne au concept une force empirique nouvelle.

par Clotilde MARCHETTI
Associée Risques extrêmes et résilience
Grant Thornton

Lex specialis (Une loi spéciale), le règlement DORA s'applique au secteur financier, entendu au sens large.

Vingt catégories d'entreprises sont concernées : établissements financiers, sociétés d'assurance, sociétés de gestion... La vingt et unième catégorie concerne les prestataires informatiques de ces entités financières, qui leur proposent des technologies et des services portant sur les systèmes d'information et de communication et adossés à leurs activités critiques.

Le règlement est en vigueur depuis janvier 2023; les entités financières assujetties devront se mettre en conformité avec ce règlement d'ici le 17 janvier 2025.

Ce calendrier prévoit un ensemble de modalités techniques d'application, à savoir des textes de niveaux 2 et 3, qui vont paraître entre janvier et juillet 2024. Des pénalités s'appliqueront en cas de non-conformité, lesquelles sont déjà précisées pour les prestataires informatiques.

Les raisons d'être du DORA

Le règlement DORA trouve son origine dans la prise de conscience que la lutte contre les attaques cyber ne peut se limiter au niveau du seul périmètre d'une entreprise, voire d'un pays. Une telle riposte se décline à l'échelle de toute l'Union européenne de manière coordonnée, et ce, pour deux raisons :

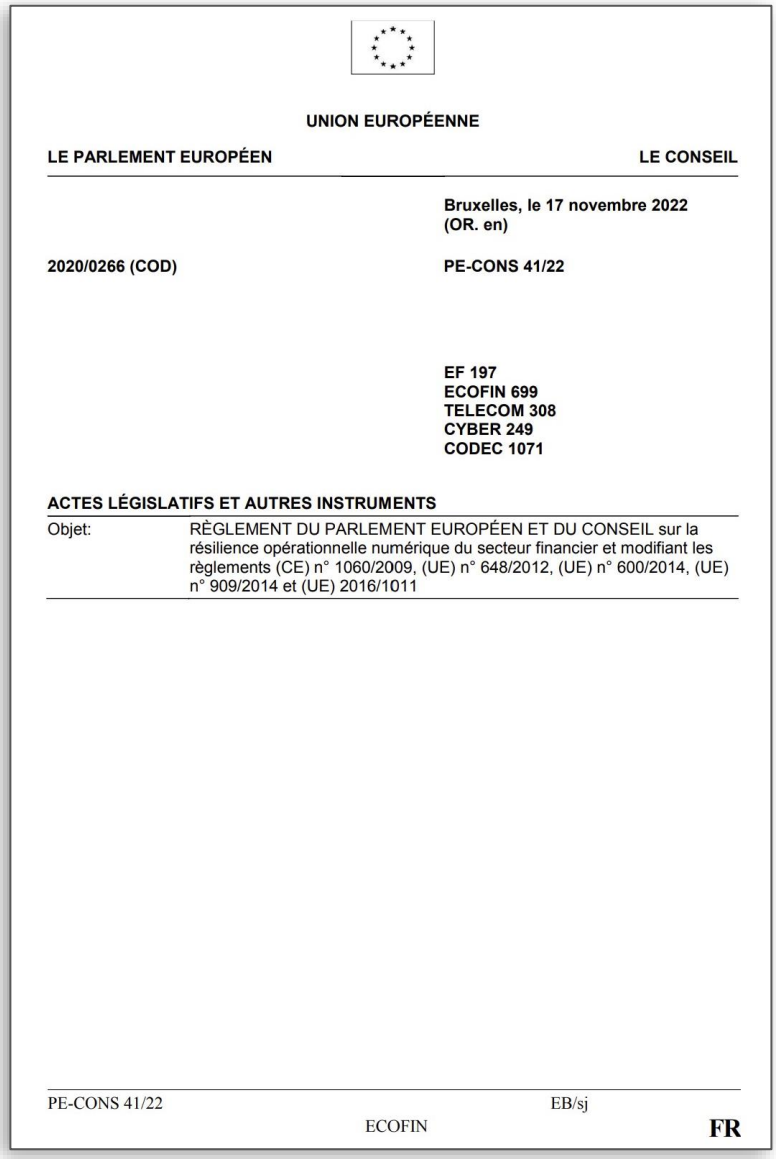
- D'abord, parce que la menace cyber est, année après année, le top risk (risque principal) exposant les organisations. Les attaquants sont organisés, voire quasi professionnalisés; ils se parlent entre eux. Leurs modes opératoires exploitent les failles technologiques et se renouvellent de manière à être toujours plus rapides et sophistiqués. Leurs moyens sont significatifs. Leurs actions sont engagées à distance et bénéficient des vides juridiques de certains États.
- Ensuite, parce que les entreprises ont elles-mêmes recours à des pratiques qui les rendent vulnérables. Parmi elles, il y a la place prépondérante qu'occupent désormais les prestataires informatiques qui fournissent les technologies en lien avec les opérations financières ou différents services en cloud (services infonuagiques).

Face au risque, il était urgent de mettre en œuvre une symétrie de la maîtrise, à savoir déployer des actions de réponse en matière à la fois d'organisation, de renforcement des capacités, de rapidité et de souplesse d'exécution, de communication et de contrôle des tiers. C'est ce qu'on appelle la résilience.

La résilience selon le DORA

Plus précisément, le règlement DORA définit la résilience opérationnelle numérique comme :

« … la capacité d'une entité financière à construire, assurer et contrôler son intégrité et sa fiabilité opérationnelle en garantissant, directement ou indirectement par le recours à des services fournis par des prestataires de services informatiques, l'ensemble des ressources nécessaires pour assurer la sécurité du réseau et des systèmes d'information qu'une entité financière utilise, et qui soutiennent la continuité des services financiers et leur qualité, y compris pendant toute la durée des perturbations… » (article 3).



UNION EUROPÉENNE

LE PARLEMENT EUROPÉEN — LE CONSEIL

Bruxelles, le 17 novembre 2022
(OR. en)

2020/0266 (COD) — PE-CONS 41/22

EF 197
ECOFIN 699
TELECOM 308
CYBER 249
CODEC 1071

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet: RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

PE-CONS 41/22 — EB/sj
ECOFIN — FR

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

sur la résilience opérationnelle numérique du secteur financier
et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012,
(UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

Cette définition de la résilience se veut plus large que celle de la sécurité globale.

Elle a l'ambition de pérenniser dans la durée différentes solutions techniques, matérielles et organisationnelles avec l'objectif de maintenir l'activité financière.

Elle implique également tout un ensemble d'acteurs à un niveau transversal, dont les prestataires de services informatiques, qui se présentent à la fois comme à l'origine de certaines vulnérabilités et comme parties prenantes des solutions de mitigation.

Les exigences du DORA

Le DORA prévoit quatre piliers successifs, qui structurent un dispositif cohérent :

- Pilier 1 : Gestion des risques informatiques et gouvernance;
- Pilier 2 : Gestion des incidents informatiques;
- Pilier 3 : Programme de tests de résilience;
- Pilier 4 : Gestion des prestataires de services numériques.

La communication aux autorités constitue un fil rouge, commun à ces grands thèmes à la fois sur la partie prévention et sur la partie gestion de l'incident.

Pour la plupart des entreprises concernées, les exigences prévues par le DORA sont déjà connues et constituent un socle de protection générique. Le DORA n'impose finalement que de renforcer ou de formaliser ce qui existe déjà.

Vers une qualification commune de ce qu'est une crise cyber

Le DORA introduit toutefois une innovation majeure. Il s'agit de la classification harmonisée au niveau de l'Union européenne de ce qu'est ou de ce que n'est pas un événement critique, en fonction de seuils définis.

Cela signifie que les entités financières disposeront désormais de la même grille de lecture de ce qu'est un incident ou une menace cyber en fonction de ses impacts – et donc décideront d'activer ou non une cellule de crise en fonction de ces mêmes critères communs.

Cette approche permet d'apporter des réponses adaptées et coordonnées à l'échelle européenne, mais elle limite aussi en interne la part de subjectivité liée à la qualification, qui résulte de considérations stratégiques ou d'appétence à la crise.

Dans les prochaines semaines, le règlement DORA va nécessiter, pour les entités financières sur le territoire européen et leurs prestataires informatiques, un travail de formalisation et de valorisation de leurs dispositifs de résilience.

C'est pourquoi il importe de bien mesurer d'ores et déjà les attendus des autorités et de tout l'écosystème afin de mieux s'approprier l'exigence de la résilience.

Clotilde Marchetti Associée Risques extrêmes et résilience - Grant Thornton

Docteure en science politique, Clotilde a commencé son parcours professionnel au sein de la préfecture de police à Paris. Elle accompagne depuis plus de 20 ans les entreprises dans la gestion de leurs crises et de leur continuité d'activité.

À lire, pour en savoir plus…

Établir un gap analysis (analyse des écarts) du DORA

Dans la mesure où le DORA renforce une situation existante, il est recommandé de déterminer les écarts entre le dispositif actuel et les exigences imposées par les autorités. Pour ce faire, un questionnaire fondé sur les dispositions réglementaires permet utilement de déterminer le niveau de maturité de l'entité.

Nous préconisons de ne pas retenir de réponses à ce questionnaire telles qu'« inexistant », « réalisé » ou encore « en cours », qui s'inscrivent dans une logique de gestion de projet. Nous considérons la logique de conformité comme plus pertinente avec une évaluation :

1) « non conforme »;
2) « majoritairement non conforme »;
3) « majoritairement conforme »;
4) « totalement conforme ».

À chacun de ces seuils, un descriptif ad hoc peut être apporté afin de mieux orienter les équipes opérationnelles. À la question, par exemple, « existe-t-il une politique de protection de l'information incluant une classification des informations sensibles, des procédures de gestion des droits d'accès, une cartographie des actifs informationnels? » (articles 8 et 9 du DORA), l'entité aura la latitude suivante :

1) La politique n'a pas été formalisée;
2) La politique a été formalisée ou partiellement formalisée;
3) La politique a été formalisée et approuvée par la gouvernance;
4) La politique a été formalisée et approuvée, et elle est révisée périodiquement.

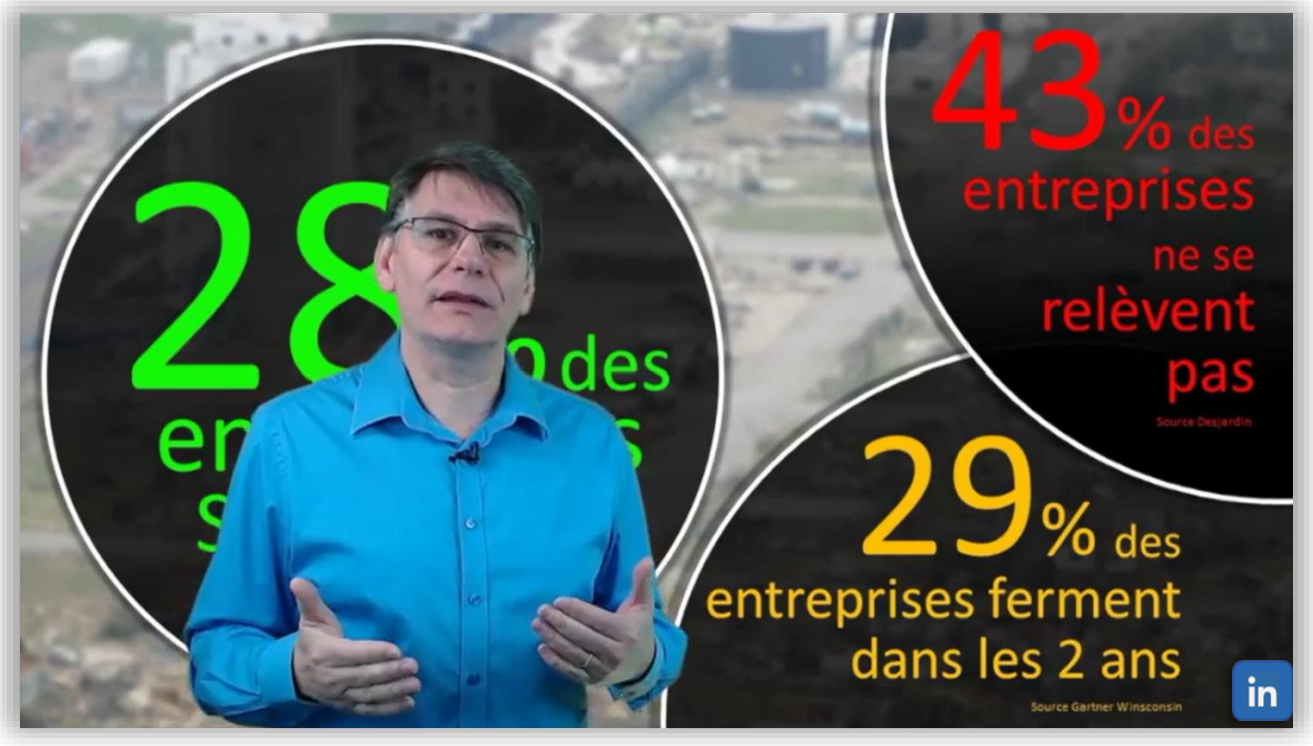
Cette approche adaptée permet de disposer de résultats chiffrés favorisant un véritable scoring (score, évaluation) à l'instant T de la maturité de l'entité financière et donc de fixer au mieux la stratégie de mise en conformité avant janvier 2025.

Invitation à Partager Votre Expertise !

Envoyez-nous un résumé de votre proposition d'article à **info@crise-resilience.com**. Les sujets tels que la continuité des activités, la gestion de crise, la communication de crise, l'intelligence économique, la sécurité civile, la gestion des risques, et la reprise informatique sont particulièrement les bienvenus.

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.



Le plan de continuité d'activité
Dernier rempart pour maintenir votre activité

FORMATIONS GRATUITES

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

Quelle place pour la communication dans une gestion de crise?

La communication n'est pas un gadget qui peut ponctuellement rendre quelques services dans la gestion d'une crise. Ce n'est pas non plus la solution miracle qui va régler toutes les difficultés rencontrées. C'est résolument un outil opérationnel, comme d'autres, qui va contribuer à résoudre la crise. Pour cela, la communication doit être mise en œuvre avec une posture proactive et donc ne pas être perçue comme un outil réactif.

par Olivier DESTEFANIS

Consultant stratégie de communication
et communication de crise

« La com, vous me préparez un communiqué de presse et un « Tweet »… ».

Trop souvent, cette phrase résume les directives données à la cellule communication lors d'un briefing (breffage) de gestion de crise.

Elle illustre parfaitement le rôle limité et réactif que l'on alloue à la fonction communication dans la conduite d'un plan de continuité des affaires. Cette position conduit inexorablement les actions communicationnelles dans une logique « outil » et en limite grandement l'efficacité.

Si cette option est choisie, c'est que, bien souvent, les acteurs de la gestion de crise se focalisent sur le court terme et la gestion de l'urgence.

Or la communication est une fonction opérationnelle puissante pour peu qu'elle soit utilisée à bon escient. Mais pour cela, la cellule communication doit impérativement adopter une position proactive.

Cela signifie qu'il est indispensable pour le communicant de réfléchir avec une vision stratégique de la situation. À l'instar de la citation de Clausewitz, il s'agit de « ne pas faire un pas sans réfléchir au dernier ».

Concrètement, la cellule communication va concevoir ses actions dans le seul but d'atteindre des objectifs et non d'activer des outils.

Prenons à titre d'exemple concret la gestion d'un incendie sur un site industriel de fabrication de produits chimiques.

L'intégrité physique des habitants n'étant plus assurée, le directeur des opérations décide de faire évacuer la population dans une zone géographique définie.

La cellule communication peut alors se contenter d'un « Tweet » informatif et d'un communiqué de presse et espérer que le plus grand nombre d'habitants concernés soit informé.

Elle peut aussi prendre le temps nécessaire pour analyser la situation. Quelle est la typologie sociologique et géographique de la zone concernée?

Transmettre une alerte d'évacuation n'a pas les mêmes répercussions dans une zone urbaine que dans une zone rurale ou que dans une zone industrielle.

Quelles vont être les conséquences de la diffusion de l'alerte? Diffuser une alerte dans une zone à forte densité d'habitants risque de provoquer rapidement une saturation des axes routiers.

À l'instar de ce qui est fait pour une opération de communication classique, cette analyse va permettre au chef de la cellule communication d'élaborer un ou des objectifs pour appuyer l'action des équipes opérationnelles lors de l'évacuation.

Cette analyse se poursuivra par l'identification des parties prenantes concernées par cet objectif, la détermination des actions à mettre en œuvre et la planification.

Ce n'est que lorsque toutes ces étapes auront été franchies que l'on étudiera les outils mobilisables, sans oublier de se fixer des indicateurs de mesure. Pour atteindre un niveau d'efficience satisfaisant des opérations de communication, trois prérequis doivent être respectés. L'expérience montre que, s'ils peuvent apparaître comme une évidence, ils sont peu souvent atteints.

"Ne pas faire un pas sans réfléchir au dernier. "

Carl von Clausewitz

Le premier prérequis est de donner les moyens au chef de la cellule communication de remplir sa mission. Cela implique de mobiliser des moyens en ressources humaines suffisants pour conduire les opérations indispensables et aussi pour tenir dans la durée si la crise perdure. En effet, concevoir une stratégie communicationnelle, gérer la pression médiatique et assurer une veille des réseaux sociaux nécessitent du personnel en nombre suffisant.

Inutile d'ajouter que ce personnel doit être formé et entraîné à la communication de crise. Il s'agit aussi de donner les moyens matériels adaptés à la mission : moyens informatiques, liaisons téléphoniques. Un placard à balais n'est pas un lieu propice pour concevoir une stratégie communicationnelle.

Le deuxième prérequis est d'établir, dès le début de la crise, une relation étroite entre le directeur des opérations et son chef de la cellule communication. Le communicant a besoin de connaître en profondeur tous les aspects de la situation. Il est aussi indispensable que le chef de la cellule soit informé en permanence des directives données par le directeur des opérations et de ses effets sur le terrain.

Enfin, le dernier prérequis est celui de l'anticipation. La coordination entre la conduite opérationnelle et celle de la communication ne s'improvise pas au déclenchement de la crise. Il faut s'y préparer. Les équipes de communication ne peuvent pas découvrir leur mission au lancement de la crise. Pour cela, des procédures doivent être établies en période propice. Ces procédures seront éprouvées lors d'exercices de gestion de crise.

La gestion d'une crise ne se résume pas à une série d'actions opérationnelles. Elle implique une communication stratégique, proactive et intégrée. Loin d'être un simple "outil", la communication joue un rôle central dans la gestion et la résolution efficaces des crises.

En adoptant une vision à long terme, en anticipant les besoins et en établissant des canaux de communication solides, la cellule de communication de crise sera à même de proposer un appui direct des opérations de gestion de crise.

Les crises sont, par nature, imprévisibles et souvent chaotiques, mais avec une communication bien planifiée et proactive, les décideurs pourront naviguer dans ces moments difficiles avec plus de liberté d'action. Il est donc indispensable de se former et de s'entrainer en période calme.

Fonctions indispensables dans une cellule de crise

Chef de cellule

Il a pour responsabilité de proposer une stratégie communicationnelle et d'en conduire les opérations. Il est en permanence en contact avec le centre des opérations pour avoir une vision précise de la situation et des directives données par le directeur des opérations.

Veille média

La veille média doit supporter l'ensemble des canaux de diffusion de l'information. Cette veille doit conduire à informer le centre opérationnel sur les évolutions des perceptions des parties prenantes au regard de la situation et sur la perception des mesures prises pour gérer la crise.

Responsable de l'animation des réseaux sociaux

Sa mission sera d'assurer la gestion des réseaux sociaux. A contrario de ce qui se fait en temps normal, la production et la veille sont permanentes. Les community managers (gestionnaires de communauté) peuvent utilement alimenter la veille média.

Gestion des relations de presse

Cette fonction va gérer l'alimentation en information des organes de presse classiques. Si la crise est complexe et à forte visibilité publique, la pression médiatique de la presse va être très forte.

Olivier Destefanis a forgé son expertise en communication de crise sur la participation à de nombreuses cellules de communication de crise, dont le centre interministériel de crise. Il intervient aussi dans ce domaine pour du conseil aux institutions et entreprises au profit d'ODS Communication et Crisotech. Il est aussi intervenant pour le séminaire communication de crise de l'Iscom Paris.

ARTICLE À DÉCOUVRIR

Dans un monde saturé d'informations, où la vérité est souvent plus étrange que la fiction, la confiance envers les médias en temps de crise est devenue un sujet brûlant. L'article "La Confiance en Temps de Crise : Les Médias et l'Appel à la Pensée Critique" de Québec Preppers offre une exploration approfondie de cette thématique, mettant en lumière les nuances de la confiance médiatique, les biais potentiels, et l'importance de la pensée critique et de l'éthique médiatique en temps de crise.

Contenu de l'article:

L'article commence par examiner comment les médias servent de bouée de sauvetage informationnelle en temps de crise, citant des exemples tels que la pandémie de COVID-19 et les inondations au Québec. Il explore ensuite les biais potentiels des médias, tels que les biais politiques et commerciaux, et comment ils peuvent influencer la couverture médiatique.

Il aborde également le lien entre la préparation aux catastrophes et la confiance médiatique, soulignant comment les citoyens prévoyants sont souvent plus conscients des biais médiatiques et cherchent à être autosuffisants en cas de crise. L'article discute du rôle des médias dans la propagation de la panique et souligne l'importance de la pensée critique pour éviter la panique et prendre des décisions éclairées en temps de crise.

Enfin, l'article conclut en soulignant l'importance de l'éthique médiatique et de la responsabilité des médias de rapporter les informations de manière honnête, précise, et transparente.

Pourquoi lire cet article?

•Compréhension Approfondie: Cet article offre une compréhension approfondie du rôle des médias en temps de crise, permettant aux lecteurs de naviguer de manière informée et critique dans le paysage médiatique contemporain.

•Évaluation de l'Information: Les lecteurs gagneront des insights précieux sur l'importance de la pensée critique et apprendront à évaluer rigoureusement l'information médiatique, une compétence essentielle dans le monde actuel saturé d'informations.

•Éthique Médiatique: L'article met en lumière les considérations éthiques dans la diffusion de l'information, aidant les lecteurs à comprendre les standards journalistiques et à distinguer l'information crédible de la désinformation.

•Préparation et Résilience: Les discussions sur la préparation aux catastrophes et la résilience sont particulièrement pertinentes pour ceux qui cherchent à développer une approche plus robuste et adaptative face aux crises.

•Perspectives Équilibrées: Avec une exploration des biais médiatiques et des affiliations politiques, cet article offre une perspective équilibrée et nuancée sur la confiance médiatique, permettant une réflexion plus riche et informée.

L'article de Québec Preppers est une lecture incontournable pour tous ceux qui souhaitent approfondir leur compréhension de la confiance médiatique en temps de crise et développer une approche plus critique et réfléchie de la consommation d'informations. Il offre des insights précieux et des perspectives équilibrées qui sont essentielles pour naviguer dans le monde complexe et souvent ambigu des médias contemporains. Alors, plongez dans cet article et découvrez comment vous pouvez devenir un consommateur d'informations plus informé et résilient!

Simulez en 3D votre prochaine cyberattaque!

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

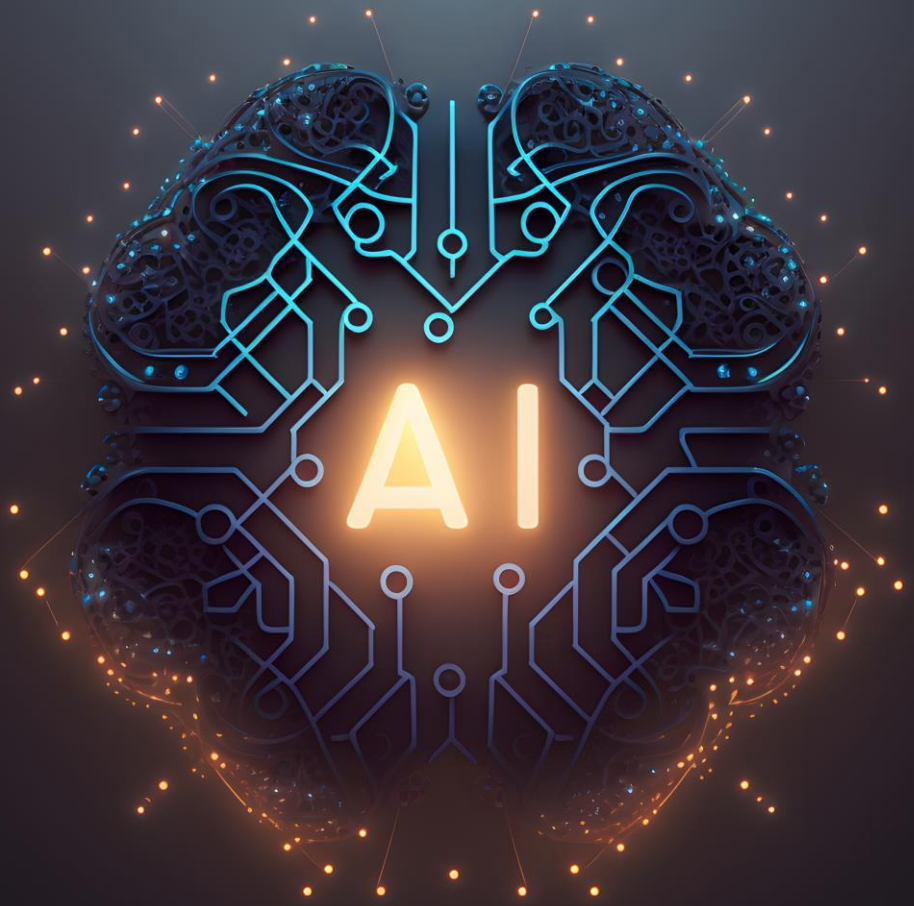
Téléchargez gratuitement 5 idées de scénarios de gestion de crise

Nous offrons GRATUITEMENT 1h de simulation de crise.

Attention le nombre de places est limité!

crise-resilience.com/simulation

Grâce à l'IA, optimisez votre gestion de crise.



Formation

INTELLIGENCE ARTIFICIELLE & GESTION DE CRISE

Apprenez à anticiper les menaces, à optimiser votre gestion de crise, à communiquer efficacement en temps de crise, et à simuler des scénarios réalistes pour une préparation optimale.

Les places sont limitées ! Agissez vite, inscrivez-vous.

https://bit.ly/3zrv3vR

En savoir plus

NE RATEZ PAS LE PROCHAIN MAGAZINE

Prochain numéro le 8 Janvier 2024

Abonnez-vous

pour recevoir le prochain magazine

www.CriseEtResilience-Magazine.com