L'ART DE SURVIVRE AUX CRISES

CRISE & RÉSILIENCE MAGAZINE

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

NUMÉRO 8 – Octobre 2024

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

Préparer les entreprises à la gestion de crise
vers une posture dérogatoire

Un employé déloyal et le bris de confiance,
ça fait très mal!

Ces plans de continuité d'activité
« théoriquement » résilients…

Cybercriminalité et compliance :
quels défis pour le secteur financier?

Audit DORA
vers une nouvelle ère de résilience digitale

Cyber
comment parler le DG couramment

DOSSIERS DU MOIS

Black-out, une menace invisible mais bien réelle

MAGAZINE OFFERT PAR CRISE & RÉSILIENCE

CRISE & RÉSILIENCE C'EST... AUSSI

Une chaîne YouTube avec...

Des conférences et formations gratuites

Des interviews d'experts :

Des réponses à vos questions :

https://www.youtube.com/criseetresilience

Une page LinkedIn avec...

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

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

Des formations ACADEMIE CRISE & RÉSILIENCE sur...

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

https://www.academiecriseetresilience.com/

Édito

Chers lecteurs,

Dans un monde en perpétuelle mutation, où les crises se succèdent et s'entrechoquent, la résilience n'est plus une option, mais une nécessité absolue. Ce numéro de Crise & Résilience Magazine vous plonge au cœur des défis contemporains qui secouent nos organisations et notre société.

L'actualité nous rappelle brutalement que nous sommes entrés dans une ère de cyberguerre larvée. Les attaques se multiplient, ciblant nos infrastructures critiques, nos entreprises et nos institutions. Face à cette menace invisible mais bien réelle, nous devons repenser notre approche de la sécurité numérique. Comme l'explique notre dossier sur les black-outs, une simple panne généralisée pourrait paralyser des pans entiers de notre économie et de notre vie quotidienne.

Mais au-delà de la simple protection, c'est toute une culture de l'antifragilité qu'il nous faut bâtir, comme le souligne notre article sur les entreprises antifragiles. Il ne s'agit plus seulement de résister aux chocs, mais d'en sortir plus fort. Cette approche novatrice irrigue l'ensemble des sujets abordés dans ce numéro, de la gestion de crise à la continuité d'activité, en passant par la cybersécurité et la compliance.

La nouvelle réglementation DORA, détaillée dans nos pages, illustre parfaitement cette volonté de renforcer la résilience opérationnelle du secteur financier face aux risques numériques. Elle impose une approche globale et proactive qui doit nous inspirer au-delà du seul domaine bancaire.

Car c'est bien l'humain qui reste au cœur de tous ces enjeux. Qu'il s'agisse de prévenir les actes de déloyauté au sein des entreprises ou de préparer nos équipes à affronter l'imprévu, le facteur humain demeure central. La résilience se construit avant tout sur la confiance, la formation et l'engagement de chacun.

Ce numéro vous offre donc un panorama complet des défis qui nous attendent et des solutions pour y faire face. Dans un monde de plus en plus incertain, Crise & Résilience Magazine reste votre boussole pour naviguer à travers les turbulences et transformer les menaces en opportunités.

Bonne lecture à tous !

L'équipe éditoriale

Partagez votre expertise dans notre magazine !

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

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

Contribuez dès maintenant à développer une culture de résilience !

L'équipe éditoriale

Direction de la publication: A.Fournier
Correction: Véronique Cyr - **Création graphique:** Alfo65 - **Crédit photo:** FreePix – Dall-E 3 – MidJourney - **Édition: C r i s e & R é s i l i e n c e -** Québec (Qc), Canada - **Nous contacter :** info@crise-resilience.com

Sommaire

Cyber : comment parler le DG couramment

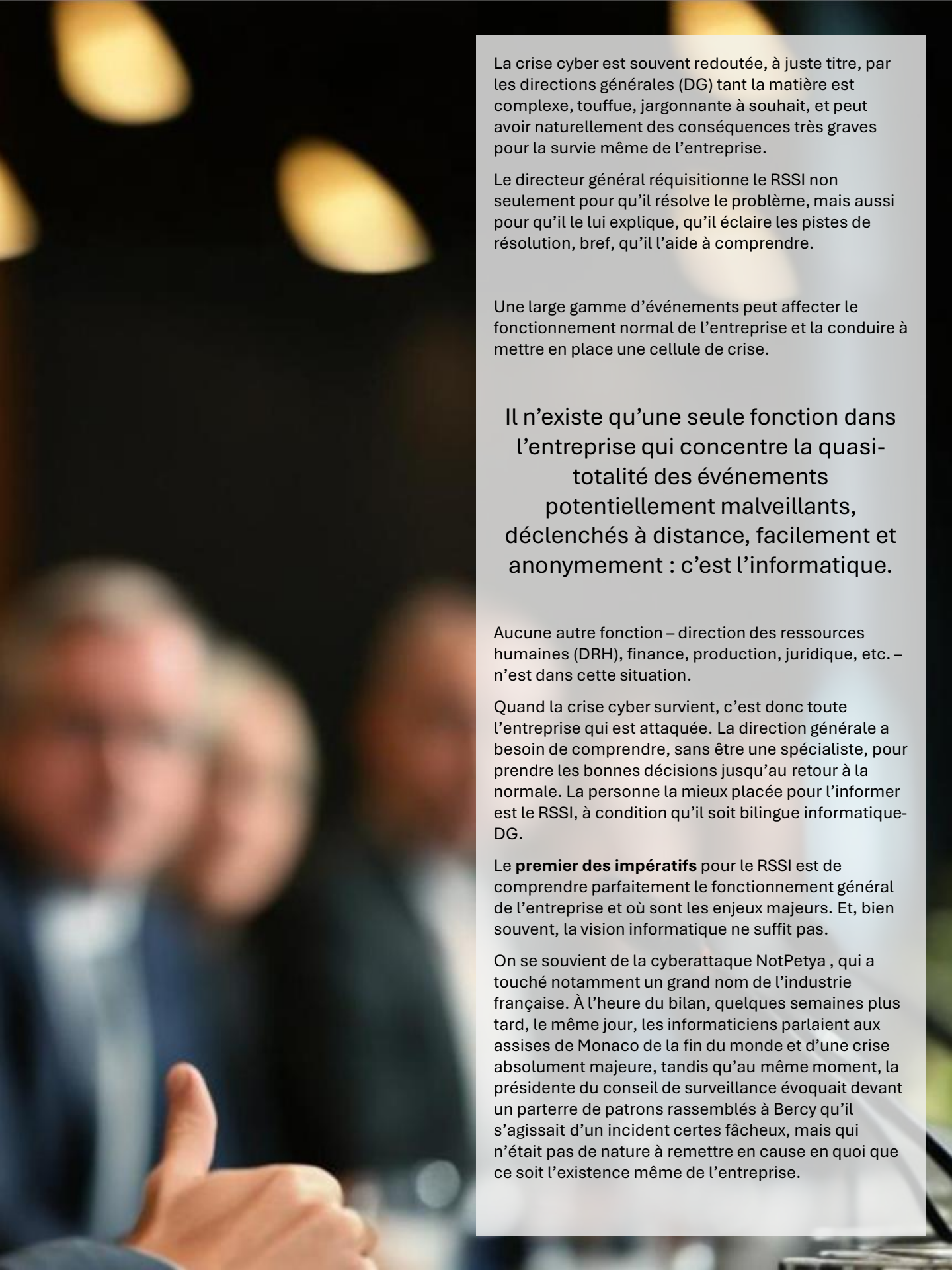
Quand une crise cyber (grave) survient, le responsable de la sécurité du système d'information (RSSI) doit se couper en deux.

Le technicien règle les problèmes et le diplomate-soutien-pour-DG-stressé monte au dernier étage.

Conseils pratiques pour rester en vie.

Par Vincent Balouet

Fondateur de Maîtrise des Crises
Analyses et recommandations en anticipation et en gestion de crises majeures



La crise cyber est souvent redoutée, à juste titre, par les directions générales (DG) tant la matière est complexe, touffue, jargonnante à souhait, et peut avoir naturellement des conséquences très graves pour la survie même de l'entreprise.

Le directeur général réquisitionne le RSSI non seulement pour qu'il résolve le problème, mais aussi pour qu'il le lui explique, qu'il éclaire les pistes de résolution, bref, qu'il l'aide à comprendre.

Une large gamme d'événements peut affecter le fonctionnement normal de l'entreprise et la conduire à mettre en place une cellule de crise.

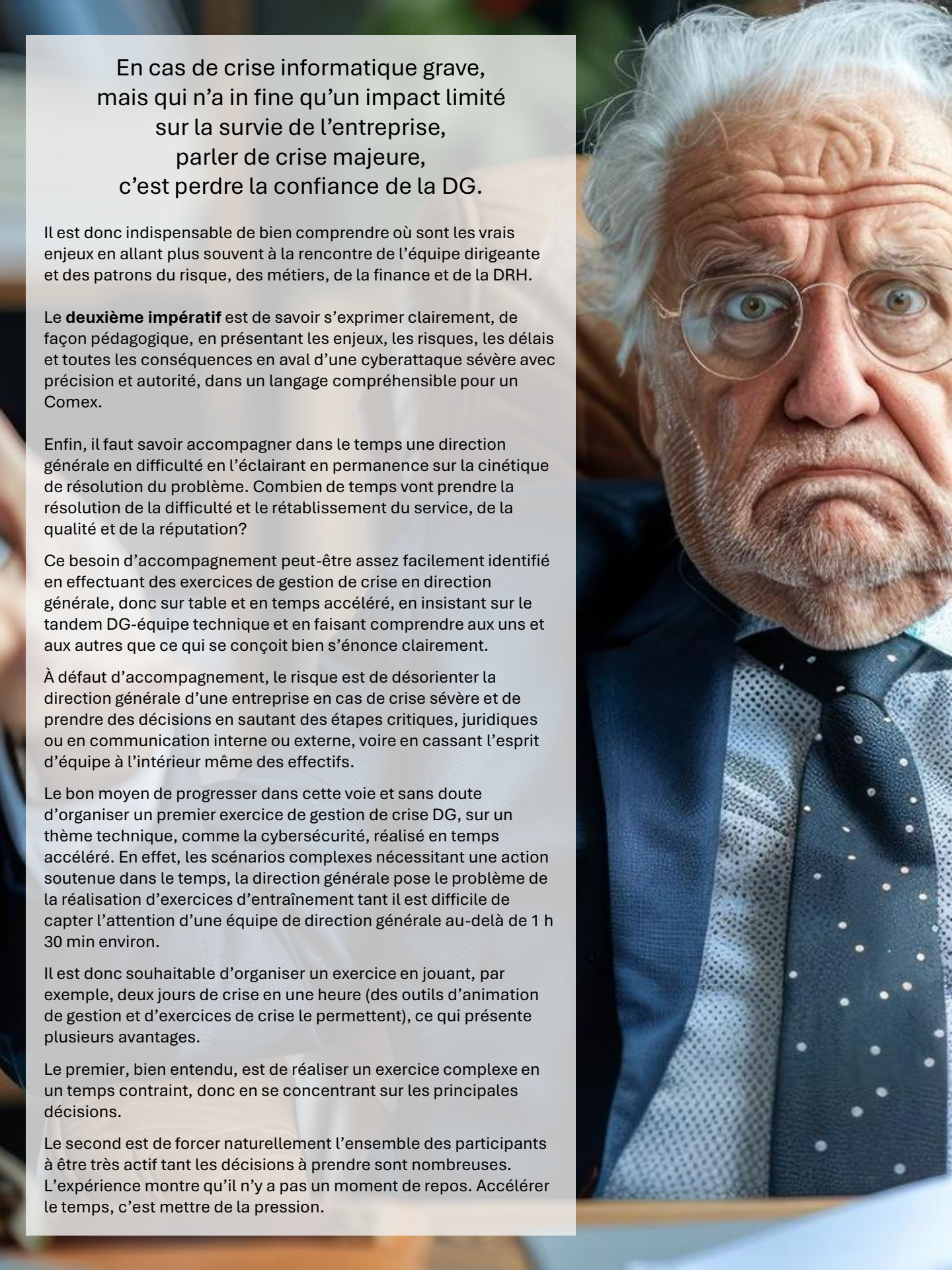
Il n'existe qu'une seule fonction dans l'entreprise qui concentre la quasi-totalité des événements potentiellement malveillants, déclenchés à distance, facilement et anonymement : c'est l'informatique.

Aucune autre fonction – direction des ressources humaines (DRH), finance, production, juridique, etc. – n'est dans cette situation.

Quand la crise cyber survient, c'est donc toute l'entreprise qui est attaquée. La direction générale a besoin de comprendre, sans être une spécialiste, pour prendre les bonnes décisions jusqu'au retour à la normale. La personne la mieux placée pour l'informer est le RSSI, à condition qu'il soit bilingue informatique-DG.

Le **premier des impératifs** pour le RSSI est de comprendre parfaitement le fonctionnement général de l'entreprise et où sont les enjeux majeurs. Et, bien souvent, la vision informatique ne suffit pas.

On se souvient de la cyberattaque NotPetya , qui a touché notamment un grand nom de l'industrie française. À l'heure du bilan, quelques semaines plus tard, le même jour, les informaticiens parlaient aux assises de Monaco de la fin du monde et d'une crise absolument majeure, tandis qu'au même moment, la présidente du conseil de surveillance évoquait devant un parterre de patrons rassemblés à Bercy qu'il s'agissait d'un incident certes fâcheux, mais qui n'était pas de nature à remettre en cause en quoi que ce soit l'existence même de l'entreprise.



En cas de crise informatique grave,
mais qui n'a in fine qu'un impact limité
sur la survie de l'entreprise,
parler de crise majeure,
c'est perdre la confiance de la DG.

Il est donc indispensable de bien comprendre où sont les vrais enjeux en allant plus souvent à la rencontre de l'équipe dirigeante et des patrons du risque, des métiers, de la finance et de la DRH.

Le **deuxième impératif** est de savoir s'exprimer clairement, de façon pédagogique, en présentant les enjeux, les risques, les délais et toutes les conséquences en aval d'une cyberattaque sévère avec précision et autorité, dans un langage compréhensible pour un Comex.

Enfin, il faut savoir accompagner dans le temps une direction générale en difficulté en l'éclairant en permanence sur la cinétique de résolution du problème. Combien de temps vont prendre la résolution de la difficulté et le rétablissement du service, de la qualité et de la réputation?

Ce besoin d'accompagnement peut-être assez facilement identifié en effectuant des exercices de gestion de crise en direction générale, donc sur table et en temps accéléré, en insistant sur le tandem DG-équipe technique et en faisant comprendre aux uns et aux autres que ce qui se conçoit bien s'énonce clairement.

À défaut d'accompagnement, le risque est de désorienter la direction générale d'une entreprise en cas de crise sévère et de prendre des décisions en sautant des étapes critiques, juridiques ou en communication interne ou externe, voire en cassant l'esprit d'équipe à l'intérieur même des effectifs.

Le bon moyen de progresser dans cette voie et sans doute d'organiser un premier exercice de gestion de crise DG, sur un thème technique, comme la cybersécurité, réalisé en temps accéléré. En effet, les scénarios complexes nécessitant une action soutenue dans le temps, la direction générale pose le problème de la réalisation d'exercices d'entraînement tant il est difficile de capter l'attention d'une équipe de direction générale au-delà de 1 h 30 min environ.

Il est donc souhaitable d'organiser un exercice en jouant, par exemple, deux jours de crise en une heure (des outils d'animation de gestion et d'exercices de crise le permettent), ce qui présente plusieurs avantages.

Le premier, bien entendu, est de réaliser un exercice complexe en un temps contraint, donc en se concentrant sur les principales décisions.

Le second est de forcer naturellement l'ensemble des participants à être très actif tant les décisions à prendre sont nombreuses. L'expérience montre qu'il n'y a pas un moment de repos. Accélérer le temps, c'est mettre de la pression.

Enfin, cette bonne pratique maintenant assez bien répandue dans les directions générales des grands groupes permet de réaliser des exercices DG sans douleur, notamment à des fins de conformité, comme l'exigeront de plus en plus les différentes réglementations touchant la gestion des risques et la cybersécurité. Ces différentes règles prennent toutes en compte la composante DG dans la gestion de crise, qui doit offrir toutes les garanties de confiance pour les certificateurs, donc les clients.

Enfin, un bon dialogue entre la direction générale et l'équipe de crise permet aussi de faire descendre le message apaisant d'une entreprise préparée, qui devient dans de nombreux cas une véritable valeur employeur très utile quand les recrutements se font de plus en plus difficiles.

La bonne compréhension des véritables enjeux au niveau de la direction générale et la clé. Seule cette compréhension permet d'éviter les faux pas, les malentendus et, en aval, les mauvaises décisions. Les différents acteurs de la crise doivent donc faire l'effort d'entrer en contact avec l'équipe de direction à froid, de s'approprier cette matière et d'élever le niveau du discours en conséquence. La direction générale accepte aussi de jouer des exercices de crise dans une forme adaptée, permettant ainsi une bonne coopération entre les différents acteurs.

Vincent Balouet

MAITRISE DES CRISES

Vincent Balouet intervient auprès des dirigeants de grandes entreprises depuis plus de 30 ans. Il a été à l'origine de la mobilisation française lors de la crise Y2k et a été appelé par le gouvernement pour fortifier la préparation générale des entreprises. Il dirige aujourd'hui maitrisedescrises.com.

www.maitrisedescrises.com

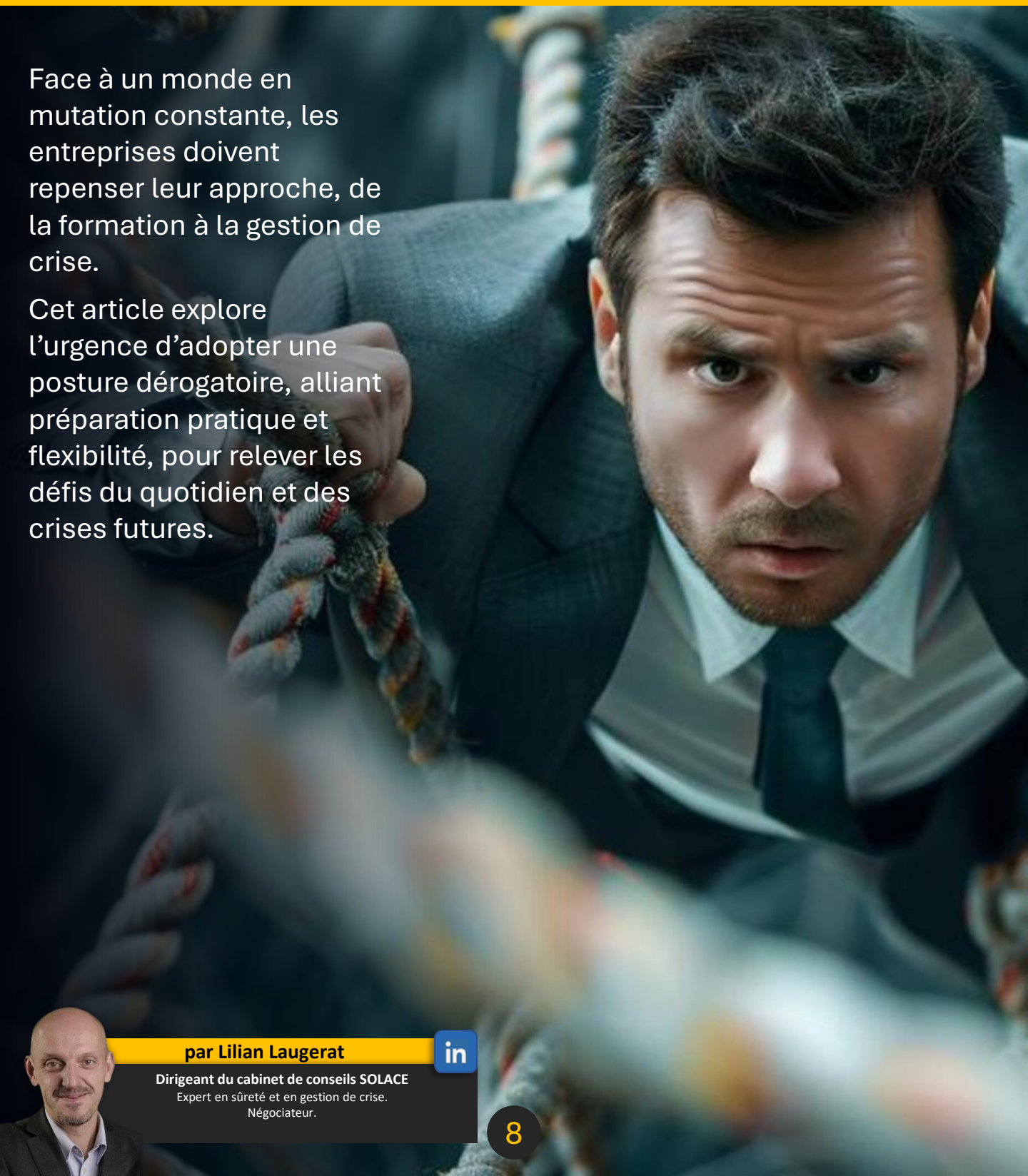
Maitrisedescrises.com est un service d'analyse et recommandations en temps réel pour les entreprises leur permettant de préparer, d'anticiper et de piloter la gestion des crises.

Pour en savoir plus, cliquer sur la vidéo.

4 recommandations pour parler le DG couramment

1. Comprendre où sont les risques et les enjeux majeurs pour l'entreprise.
2. Bien s'exprimer, avec autorité et précision.
3. Faire des exercices réguliers en direction générale en temps accéléré.
4. Profiter de ce bon fonctionnement pour mettre à profit la confiance dans l'entreprise.

Préparer les entreprises à la gestion de crise : vers une posture dérogatoire



Face à un monde en mutation constante, les entreprises doivent repenser leur approche, de la formation à la gestion de crise.

Cet article explore l'urgence d'adopter une posture dérogatoire, alliant préparation pratique et flexibilité, pour relever les défis du quotidien et des crises futures.

par Lilian Laugerat

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

Dans un environnement en perpétuelle évolution, les crises sont inévitables.

Plutôt que de se contenter de formations traditionnelles, les entreprises doivent adopter une posture dérogatoire, se préparant à l'imprévu avec des méthodes pratiques et flexibles, essentielles pour naviguer avec succès à travers les turbulences de demain.

La réalité des crises dans un monde en mutation

Dans un environnement où les changements sont constants, les crises, qu'elles soient économiques, sanitaires, technologiques ou climatiques, représentent une menace omniprésente pour les entreprises. L'impact de la crise sanitaire de la COVID-19, qui a surpris de nombreuses organisations, met en lumière l'importance d'une préparation adéquate. La gestion de crise n'est pas une compétence optionnelle, mais une nécessité stratégique. Pourtant, elle est souvent perçue comme une discipline complexe nécessitant une préparation rigoureuse qui dépasse les méthodes de formation classiques.

Les limites de la formation traditionnelle

Les formations traditionnelles, souvent théoriques et limitées dans le temps, ne répondent plus aux besoins d'une préparation efficace à la gestion de crise. Les entreprises, déjà accaparées par la gestion quotidienne, considèrent souvent la formation à la crise comme une activité secondaire ne justifiant pas un investissement substantiel de temps et de ressources. Cependant, la nature imprévisible et complexe des crises exige bien plus qu'une simple formation : elle requiert une préparation continue, orientée vers l'action et intégrée dans le quotidien de l'entreprise.

Adopter une posture dérogatoire

Pour être réellement efficace, la préparation à la gestion de crise doit s'inscrire dans une posture dérogatoire, où la priorité est donnée à l'essentiel : l'action et la méthode. Cette posture dérogatoire implique de sortir du cadre classique pour se concentrer sur des exercices pratiques et réguliers qui permettent aux équipes de se familiariser avec les outils et les processus nécessaires. Ces exercices ne doivent pas être réservés aux seules situations de crise, mais devenir une partie intégrante de la gestion quotidienne. Ainsi, les collaborateurs développent une capacité réflexe à réagir, ce qui est essentiel en période de crise.

La répétition des fondamentaux : clé de la préparation

La gestion de crises ne doit rien au hasard. Pour que les décisions soient prises rapidement et efficacement, les membres de la cellule de crise doivent être habitués à travailler ensemble sous pression. Une méthode claire, répétée régulièrement dans des scénarios problématiques du quotidien, renforce leur aptitude à répondre à une véritable crise.

Ces répétitions permettent d'ancrer les réflexes nécessaires, tout en rendant la méthodologie de crise pertinente pour les défis quotidiens de l'entreprise.

Un modèle de réponse adaptable et quotidien

Lorsqu'une crise survient, elle bouleverse le fonctionnement normal de l'entreprise, nécessitant une réponse adaptée à la situation unique.

La préparation consiste donc à développer une méthode flexible, capable d'évoluer au fil des événements. Pour être réellement efficace, cette méthodologie doit être pratiquée régulièrement en dehors des situations de crise, afin que son application devienne presque instinctive.

La préparation à la gestion de crise exige une approche innovante, ancrée dans la réalité quotidienne de l'entreprise.

En adoptant une posture dérogatoire, les entreprises peuvent non seulement mieux se préparer aux crises, mais aussi améliorer leur résilience face aux défis quotidiens et aux attendus des parties prenantes.

La clé réside dans la répétition des fondamentaux et l'intégration de la méthodologie de crise dans les processus courants, permettant ainsi une réponse rapide et coordonnée lorsque la situation l'exige.

La gestion de crise impose un changement de paradigme dans la manière dont les entreprises se préparent aux événements imprévus. Il ne suffit plus de former les équipes selon des méthodes traditionnelles combinant seulement gestion des risques et communication de crise; il faut les préparer à l'action, en leur fournissant les outils, les méthodes et les réflexes nécessaires pour faire face à l'inattendu.

La préparation doit également intégrer ces méthodes dans la gestion des problèmes quotidiens, afin d'assurer leur maîtrise et leur disponibilité en temps de crise. En rendant les méthodes de gestion de crise applicables au quotidien, les entreprises créent un environnement où les équipes sont constamment prêtes à réagir face à l'imprévu.

Ce changement d'approche est aujourd'hui indispensable pour permettre aux entreprises de traverser les crises avec efficacité et de continuer à prospérer dans un environnement toujours plus incertain. Sans jamais oublier que le temps d'une gestion de crise réelle sera toujours notre meilleur professeur.

Lilian Laugerat

SOLACE

Solace est un cabinet de conseil dont l'objectif est de préparer les entreprises à faire face aux situations de gestion de crise auxquelles elles pourraient être confrontées.

www.agirpourreleverledefi.com

Application de la méthodologie dans notre quotidien

Il est crucial d'intégrer une méthodologie de gestion de crise dans les activités quotidiennes des entreprises pour les préparer efficacement à gérer des situations de crise potentielles. Elle permet d'améliorer le processus décisionnel en période de crise, ce qui est essentiel pour minimiser les impacts et répondre rapidement aux situations imprévues.

- Premièrement, l'application quotidienne de cette méthodologie permet aux entreprises de maintenir une vigilance constante. En ayant des processus de gestion de crise bien établis, les entreprises peuvent réagir plus rapidement et de manière plus structurée lorsqu'une crise survient, ce qui est vital pour limiter les dommages potentiels sur les personnes, les activités, l'image, la responsabilité et les finances de l'entreprise.
- Deuxièmement, l'utilisation régulière de cette méthodologie aide à identifier et à comprendre les parties prenantes essentielles, tant internes qu'externes, qui pourraient être affectées par une crise. Cela permet de créer un réseau de communication robuste et d'anticiper les besoins de ces parties prenantes, ce qui est crucial pour maintenir la confiance et la réputation de l'entreprise en période de turbulence.
- Enfin, en intégrant cette méthodologie dans la gestion quotidienne, les entreprises sont mieux préparées à élaborer et à exécuter des plans d'action efficaces en cas de crise. Cela inclut la définition de responsabilités claires, la priorisation des actions et le suivi constant de leur mise en œuvre, garantissant ainsi une réponse rapide et cohérente.

En somme, utiliser la méthodologie au quotidien permet aux entreprises de renforcer leur capacité, d'améliorer leur réactivité face aux crises et de protéger leurs intérêts stratégiques à long terme.

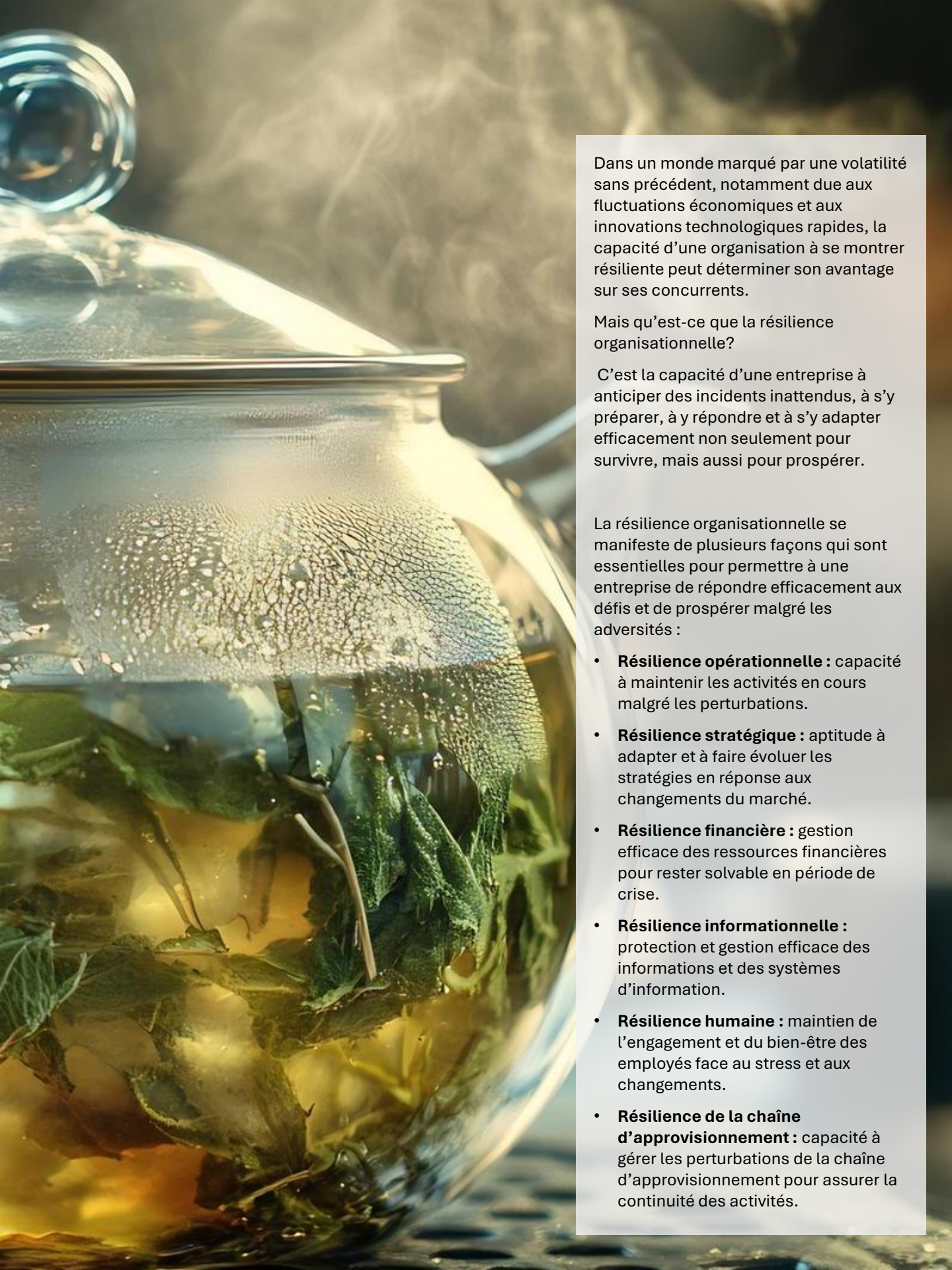
Résilience en action! Infuser la capacité de rebondir dans la culture d'entreprise

La résilience est indispensable pour toute entreprise qui souhaite durer. Mais par où commencer pour intégrer cette force au cœur de votre organisation?

Découvrez nos secrets pour faire de la résilience votre alliée au quotidien, et ce, malgré les défis.

Par Karine Maréchal-Richard

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



Dans un monde marqué par une volatilité sans précédent, notamment due aux fluctuations économiques et aux innovations technologiques rapides, la capacité d'une organisation à se montrer résiliente peut déterminer son avantage sur ses concurrents.

Mais qu'est-ce que la résilience organisationnelle?

C'est la capacité d'une entreprise à anticiper des incidents inattendus, à s'y préparer, à y répondre et à s'y adapter efficacement non seulement pour survivre, mais aussi pour prospérer.

La résilience organisationnelle se manifeste de plusieurs façons qui sont essentielles pour permettre à une entreprise de répondre efficacement aux défis et de prospérer malgré les adversités :

- **Résilience opérationnelle :** capacité à maintenir les activités en cours malgré les perturbations.
- **Résilience stratégique :** aptitude à adapter et à faire évoluer les stratégies en réponse aux changements du marché.
- **Résilience financière :** gestion efficace des ressources financières pour rester solvable en période de crise.
- **Résilience informationnelle :** protection et gestion efficace des informations et des systèmes d'information.
- **Résilience humaine :** maintien de l'engagement et du bien-être des employés face au stress et aux changements.
- **Résilience de la chaîne d'approvisionnement :** capacité à gérer les perturbations de la chaîne d'approvisionnement pour assurer la continuité des activités.

Adopter une approche en 9 étapes

Introduire une culture de la résilience au sein d'une organisation requiert une stratégie bien pensée et un engagement à tous les niveaux de l'entreprise. Voici une approche en plusieurs étapes pour y parvenir efficacement :

1-Leadership de la direction : la culture de la résilience doit s'ancrer au sommet. La direction doit non seulement soutenir les initiatives de résilience, mais aussi les incarner. Les leaders doivent communiquer leur vision de la résilience de manière claire, montrant comment elle s'aligne sur les valeurs et les objectifs de l'organisation.

2-Gestion proactive des risques : avant de pouvoir renforcer la résilience, une entreprise doit comprendre les risques auxquels elle est exposée. Cela inclut l'analyse des menaces internes et externes, la compréhension des points faibles dans les activités et la préparation à faire face à des scénarios variés et évolutifs.

3-Formation et sensibilisation : éduquer et former les employés sur la résilience est essentiel. Cela peut prendre la forme de formations à la gestion de crise, de simulations de crise et d'ateliers sur la résilience mentale et émotionnelle. L'objectif est de préparer chaque membre de l'organisation à penser et à agir de manière résiliente.

4-Communication ouverte : un environnement où la communication est ouverte et encourage la remontée d'informations doit être favorisé. Les employés doivent se sentir à l'aise de faire connaître leurs préoccupations et leurs idées sur la manière d'améliorer la résilience.

5-Flexibilité et innovation : encourager l'innovation et la flexibilité peut aider les organisations à s'adapter rapidement aux changements et aux défis. Cela peut inclure l'adoption de nouvelles technologies, la modification des processus ou la redéfinition des rôles pour être plus réactif et agile.

6-Apprentissage continu : les organisations résilientes apprennent de chaque incident et adaptent leurs pratiques en conséquence. Cela implique une analyse continue de ce qui fonctionne, de ce qui ne fonctionne pas, et pourquoi.

7-Bien-être des employés : mettre l'accent sur le bien-être physique et mental, offrir des programmes de bien-être et des ressources en santé mentale et encourager un équilibre travail-vie personnelle est important. Les employés en bonne santé sont plus résilients et plus engagés.

8-Renforcement des réseaux et des partenariats : il est important de renforcer les réseaux de soutien tant internes qu'externes. Cela peut inclure le renforcement des partenariats commerciaux, l'amélioration des systèmes de soutien aux employés et la collaboration avec des organisations locales et des agences de réponse aux urgences.

9-Célébration des succès et apprentissage des échecs : reconnaître et célébrer les comportements et les initiatives renforce la culture de résilience. De même, analyser les échecs ou les défis et apprendre d'eux aide à améliorer les stratégies futures de résilience.

Surmonter les principaux obstacles

Intégrer une culture de la résilience au sein des organisations modernes présente un ensemble complexe de défis qui requièrent une attention particulière et un engagement stratégique continu.

Voici un aperçu des principaux obstacles que nous avons pu rencontrer et des réflexions sur la manière de les surmonter :

- **Résistance au changement :** l'habitude et le confort avec les routines existantes peuvent entraver l'adoption de nouvelles pratiques résilientes. L'engagement des parties prenantes et une communication claire sur les bénéfices sont essentiels pour surmonter cette résistance.
- **Manque de ressources :** le développement d'une culture de résilience nécessite des investissements en temps, en argent et en personnel. Face aux contraintes budgétaires, il est important de prioriser les investissements et d'explorer d'autres sources de financement.
- **Communication inefficace :** une mauvaise communication peut nuire à la compréhension et à l'engagement envers les objectifs de résilience. Un plan de communication efficace, y compris des rétroactions régulières et la reconnaissance des réussites, est crucial.
- **Complexité des enjeux :** les défis auxquels les organisations font face sont souvent complexes et nécessitent des stratégies adaptatives. Une analyse continue et des ajustements des plans sont nécessaires pour y répondre efficacement.
- **Maintien de l'engagement à long terme :** garder l'organisation engagée envers la résilience après la phase initiale de mise en œuvre peut être difficile. La résilience doit être constamment réévaluée et renouvelée pour rester pertinente et intégrée dans la culture organisationnelle. Elle doit intégrer l'ADN de l'entreprise.

Aux vues des changements rapides et des incertitudes accrues, surtout ces derniers mois, l'instauration d'une culture de la résilience dans les organisations est essentielle non seulement pour survivre, mais aussi pour prospérer.

Cela requiert un engagement de tous les niveaux de l'entreprise, de la direction à chaque employé.

Les défis à surmonter incluent la résistance au changement, le manque de ressources et la nécessité d'une communication efficace et continue.

Pour réussir, les organisations doivent investir dans la formation, encourager l'innovation et cultiver un environnement ouvert et flexible.

En s'engageant de façon volontaire et continue dans ces pratiques, les entreprises peuvent transformer les défis en possibilités, renforçant ainsi leur capacité à naviguer dans un avenir incertain, avec agilité, prévoyance et, bien sûr... avec résilience.

Karine Maréchal-Richard

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

www.crise-resilience.com

CRISE & RÉSILIENCE

L'ART DE SURVIVRE AUX CRISES

9 outils pratiques pour bâtir une culture de résilience

Ateliers de résolution de problèmes : organisez des ateliers où les employés peuvent collaborer pour résoudre des problèmes réels auxquels l'entreprise est confrontée. Utilisez des techniques comme le brainstorming pour encourager la créativité et l'innovation.

Jeux de simulation de crise : mettez en place des jeux de rôle ou des simulations de crise où les équipes doivent travailler ensemble pour naviguer à travers une série de scénarios. Cela peut aider à développer des compétences de prise de décision rapide et à améliorer la communication sous pression.

Séances de retour d'expérience : après chaque projet majeur ou incident critique, organisez des séances où les équipes peuvent discuter de ce qui s'est bien passé, de ce qui pourrait être amélioré et de comment appliquer ces leçons à l'avenir. Cela encourage une culture d'apprentissage continu et d'amélioration.

Activités de consolidation d'équipe : organisez des activités de renforcement d'équipe divertissantes et stimulantes pour renforcer la collaboration sous pression. Ces événements incluent des escape games et des compétitions sportives amicales visant à améliorer l'esprit d'équipe et la coopération.

Hackathons : organisez des hackathons internes où les employés peuvent proposer des innovations pour améliorer les produits ou les services de l'entreprise. Cela stimule l'engagement et la collaboration entre les équipes.

Infolettres inspirantes : créez une infolettre mensuelle qui met en avant des histoires de résilience et de succès au sein de l'organisation, des conseils de bien-être et des actualités importantes. Rendez-la visuelle et interactive pour capter l'intérêt des lecteurs. Partagez-y ce magazine, par exemple.

Programmes de mentorat : mettez en place des programmes de mentorat, par lesquels les employés plus expérimentés guident les plus jeunes ou les nouveaux employés, peut favoriser un environnement de soutien et de développement continu. Cela aide aussi à transmettre des valeurs de résilience et des compétences clés à travers l'organisation.

Forums de retroactions : établissez des forums réguliers où les employés peuvent exprimer librement leurs idées, leurs préoccupations et leurs suggestions. Cela peut être facilité par des plateformes en ligne ou des réunions en face à face.

Infographies sur la résilience : produisez des infographies attrayantes qui fournissent des données et des conseils sur la résilience. Elles peuvent être partagées sur les intranets de l'entreprise ou par les réseaux sociaux internes pour maximiser la visibilité.

ABONNEZ-VOUS Gratuitement

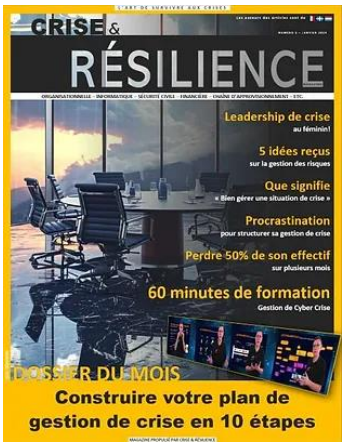
TRIMESTRIEL – JANVIER – AVRIL – JUILLET – OCTOBRE

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

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 un 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!



Abonnez-vous sur www.criseetresilience-magazine.com

La chaîne YouTube Crise & Résilience

Des conférences et formations gratuites

Des interviews d'experts :

27-28 NOVEMBRE 2024 | PARIS, PORTE DE VERSAILLES

L'ÉVÉNEMENT DES PROFESSIONNELS DE LA CYBER

Cloud & Cyber Security Expo réunit leaders de l'industrie avec pour objectif de s'instruire, partager, innover et générer des opportunités.

Découvrez les solutions innovantes d'entreprises telles que **Wiz**, **Threatlocker**, **Box**, **Scafe**, **Aqua Security** et bien d'autres.

Un programme exceptionnel vous attend avec des intervenants de renom pour discuter des enjeux du secteur :

- Comment l'IA révolutionne la cybersécurité
- La cybersécurité sectorielle : les défis par industrie
- La sécurité du cloud
- Les facteurs humains
- L'évolution des menaces : comment s'adapter ?

Un rendez-vous à ne pas manquer pour tous les acteurs du cloud et de la cybersécurité

+ de 6 200 visiteurs | + 255 exposants I + de 290 conférenciers

RETIREZ VOTRE BADGE GRATUIT

CLOUD & CYBER SECURITY EXPO

TECH SHOW PARIS
techshowparis.fr

REGROUPANT

CLOUD EXPO EUROPE | DEVOPS LIVE | CLOUD & CYBER SECURITY EXPO | BIG DATA & AI WORLD | DATA CENTRE WORLD

L'ÉVÈNEMENT DÉDIÉ AUX PROFESSIONNELS DE LA TECH EN FRANCE

ORGANISÉ PAR

CloserStill

Black-out, une menace invisible, mais bien réelle!

Et si tout s'arrêtait d'un coup ?

Plus de lumière, plus d'internet, plus de communication.

C'est le scénario redouté d'un black-out électrique ou informatique.

Une menace bien réelle qui pourrait paralyser nos infrastructures essentielles en un instant.

Face à l'augmentation des cyberattaques et aux risques grandissants, êtes-vous prêt à affronter l'impensable ?

Interview 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.

Imaginez un instant... tout s'arrête.

Plus de lumière, plus d'ordinateurs, plus de réseaux.

Le silence numérique et l'obscurité totale.

Ce scénario, c'est ce qu'on appelle un black-out. Qu'il soit électrique ou informatique, les conséquences sont rapides et peuvent être dévastatrices.

Un black-out électrique, c'est lorsque l'alimentation en électricité disparaît sur de vastes zones, paralysant tout, des transports aux hôpitaux, jusqu'aux entreprises qui dépendent du moindre watt pour fonctionner.

Rien ne bouge. Plus rien ne fonctionne.

Un black-out informatique, lui, survient lorsque nos systèmes numériques cessent de répondre. Souvent déclenché par des cyberattaques ou des pannes techniques majeures, il touche directement nos infrastructures critiques : communications, banques, gestion des services publics. Le chaos s'installe.

Et le pire ?

Ces deux phénomènes peuvent se conjuguer, créant un effet domino dévastateur. La communication s'effondre, l'économie vacille, et la sécurité publique est mise à rude épreuve.

Êtes-vous prêt pour un tel scénario ?

Pourquoi ce sujet est-il crucial aujourd'hui ?

Nous vivons dans un monde où les infrastructures électriques et informatiques sont devenues les piliers de notre société moderne. Mais elles sont aussi des cibles privilégiées des cyberattaques. Que ce soit pour des raisons financières ou des actes de cyberterrorisme, ces menaces visent directement les infrastructures critiques.

Imaginez une cyberattaque qui plonge des villes entières dans l'obscurité ou un black-out informatique qui paralyse le fonctionnement des gouvernements et des entreprises. Ces scénarios ne sont plus de simples hypothèses, mais des réalités actuelles qui menacent la stabilité des nations.

Notre **HYPER dépendance** à la technologie, aux systèmes interconnectés, aux IA, amplifie cette vulnérabilité.

Chaque entreprise, chaque gouvernement doit se poser une question simple mais vitale :

Sommes-nous réellement prêts à faire face à un black-out ?

> “ Aujourd'hui, se préparer n'est plus une option, c'est une nécessité. ”
>
> *Alexandre Fournier*

1. LES RISQUES ET SCÉNARIOS DE DÉCLENCHEMENT

Lorsqu'on parle de black-out, il est essentiel de comprendre qu'il existe plusieurs types d'interruptions qui peuvent paralyser nos infrastructures critiques.

Qu'il s'agisse d'une panne électrique ou d'une défaillance des systèmes informatiques, les conséquences peuvent varier en fonction de l'ampleur et de la nature du black-out.

Dans certains cas, l'interruption peut être totale, touchant de larges zones géographiques et affectant simultanément plusieurs secteurs.

D'autres fois, elle sera partielle, limitée à certaines régions ou infrastructures spécifiques, mais tout aussi perturbatrice.

Cette distinction est cruciale car elle influence directement les stratégies de réponse à mettre en place et la durée nécessaire pour rétablir une situation normale.

TYPES DE BLACK-OUT

Black-out total vs partiel

Un **black-out total** implique l'interruption complète de l'électricité et/ou des systèmes informatiques sur une large zone, tandis qu'un **black-out partiel** ne touche que certaines régions ou infrastructures spécifiques.

La portée de ces incidents influence directement les stratégies de réponse et la durée de rétablissement.

Un **black-out prolongé** peut déclencher des effets domino, impactant des secteurs critiques comme la santé, les transports et la sécurité publique. Par exemple, une panne d'électricité prolongée peut stopper les systèmes hospitaliers, mettant en danger les patients en soins intensifs, ou paralyser les transports publics, empêchant les déplacements des travailleurs essentiels.

De même, un **black-out informatique** pourrait perturber les chaînes d'approvisionnement, rendant les systèmes de gestion des stocks et de distribution inaccessible.

Ces effets en cascade soulignent l'importance cruciale de renforcer la résilience et de mettre en place des mesures de préparation adaptées pour prévenir une déstabilisation complète de la société.

Électrique vs informatique

Les **blackouts électriques** perturbent l'approvisionnement en énergie, tandis que le **blackout informatique** affecte la disponibilité des systèmes numériques, souvent à cause de cyberattaques, de pannes ou d'erreurs humaines.

Ces deux types de black-out sont interdépendants : un black-out électrique peut provoquer des pannes informatiques, et inversement.

SOURCES POTENTIELLES DE BLACK-OUT

Les black-out peuvent avoir plusieurs origines, qu'elles soient naturelles, humaines ou technologiques. Chacune de ces causes présente des caractéristiques uniques qui influencent l'ampleur des dommages et la rapidité des réponses nécessaires.

Identifier ces sources potentielles est essentiel pour se préparer à anticiper et limiter les effets dévastateurs de ces incidents.

Attaques de type cyberterrorisme et cyber guerre

Les cyberattaques ciblant des infrastructures critiques sont devenues une menace majeure à l'échelle mondiale.

Qu'il s'agisse d'attaques techniques comme des ransomwares, des malwares, ou des intrusions visant à prendre le contrôle des réseaux électriques et des systèmes numériques, ces menaces peuvent causer des blackouts à grande échelle.

Les cybercriminels, les groupes de cyberterroristes et les États-nations utilisent ces attaques pour différentes raisons : perturber l'économie, exercer une pression géopolitique, ou semer la terreur. Le cyberterrorisme et la cyber guerre sont des stratégies utilisées pour fragiliser des sociétés sur le long terme, attaquant à la fois les infrastructures énergétiques et informatiques.

Actions malveillantes (terrorisme, sabotage)

En plus des cyberattaques, les actions malveillantes telles que le sabotage physique de centrales électriques ou de lignes de transmission représentent une menace directe pour l'alimentation en énergie et les systèmes informatiques.

Ces attaques physiques peuvent provoquer des black-out prolongés avec des conséquences dévastatrices pour les infrastructures critiques.

Incidents naturels

Les phénomènes naturels tels que les tempêtes solaires et les événements climatiques extrêmes (tempêtes, ouragans, inondations) peuvent également provoquer des blackouts.

Ces événements climatiques endommagent non seulement les réseaux électriques mais aussi les systèmes de communication, rendant les interventions de secours encore plus difficiles.

Erreurs humaines et dysfonctionnements systémiques

Les erreurs humaines et les défaillances des systèmes de gestion de l'énergie peuvent provoquer des black-out non intentionnels.

Des infrastructures vieillissantes, un manque de maintenance adéquate, ou une mauvaise manipulation des systèmes peuvent entraîner des pannes majeures.

2. IMPACTS SUR LES PRINCIPAUX PANS DE LA SOCIÉTÉ

Un black-out ne se contente pas de plonger des régions dans l'obscurité ou de paralyser les systèmes numériques.

Ses répercussions s'étendent bien au-delà, affectant profondément les infrastructures critiques, les services publics, et même notre capacité à communiquer.

Ces incidents révèlent à quel point nos sociétés modernes sont interdépendantes et fragiles face à ces perturbations massives. Comprendre ces impacts est essentiel pour mieux se préparer et renforcer notre résilience face à ces crises.

INFRASTRUCTURES CRITIQUES

Réseaux de transport (routier, ferroviaire, aéroportuaire)

Lors d'un black-out, les réseaux de transport se retrouvent en grande difficulté. Les feux de circulation s'éteignent, provoquant des embouteillages massifs et des accidents. Sur les voies ferrées, les trains s'immobilisent, laissant des passagers bloqués pendant des heures. Les aéroports ne sont pas épargnés : les systèmes de gestion des vols et le contrôle aérien sont perturbés, entraînant des annulations, des retards, voire des fermetures d'aéroports.

Le chaos dans les transports peut rapidement affecter l'ensemble de l'économie et perturber les chaînes d'approvisionnement.

Services de santé (hôpitaux, urgentistes)

Les hôpitaux dépendent d'une alimentation électrique stable pour maintenir les équipements vitaux en fonctionnement. En cas de black-out, les générateurs de secours prennent le relais, mais leur autonomie est limitée. Si l'interruption dure trop longtemps, la vie des patients en soins intensifs ou sous traitement critique est mise en danger.

De plus, les services d'urgence peuvent être débordés par l'afflux d'appels, rendant la gestion des ressources encore plus complexe.

Énergie (répartition et interruptions)

La gestion de l'énergie résiduelle devient un défi majeur en période de black-out. La répartition doit se faire avec précaution pour éviter toute surcharge. Les infrastructures critiques, comme les hôpitaux et les services d'urgence, sont priorisées.

Cependant, des pannes prolongées peuvent entraîner des pénuries énergétiques qui durent plusieurs semaines, aggravant encore la situation.

ÉDUCATION ET SERVICES PUBLICS

Fermeture d'écoles et interruption des services éducatifs

L’absence d’électricité contraint souvent les établissements scolaires à fermer leurs portes.

Les activités pédagogiques ne peuvent plus être assurées, faute de chauffage, d’éclairage ou d’équipements informatiques.

Les cours en ligne sont également compromis par l'indisponibilité des réseaux, mettant en péril la continuité de l'éducation et laissant des milliers d’élèves sans accès à l'apprentissage.

Accès aux services administratifs

Les services publics et administratifs sont paralysés en l'absence de systèmes informatiques et d'électricité.

Les citoyens se retrouvent incapables d’effectuer des démarches importantes comme l’obtention de certificats ou le renouvellement de documents.

Ces retards, accompagnés de frustrations, peuvent engendrer des tensions au sein de la population.

COMMUNICATION

Indisponibilité des réseaux de communication (téléphone, internet)

Lors d'un black-out, les réseaux de communication sont souvent parmi les premiers à tomber. Sans électricité, les antennes relais cessent de fonctionner, coupant les communications téléphoniques et l'accès à internet.

Cela isole des millions de personnes et limite considérablement la capacité des autorités à coordonner les secours ou à transmettre des informations cruciales.

Impacts sur la transmission d’informations cruciales

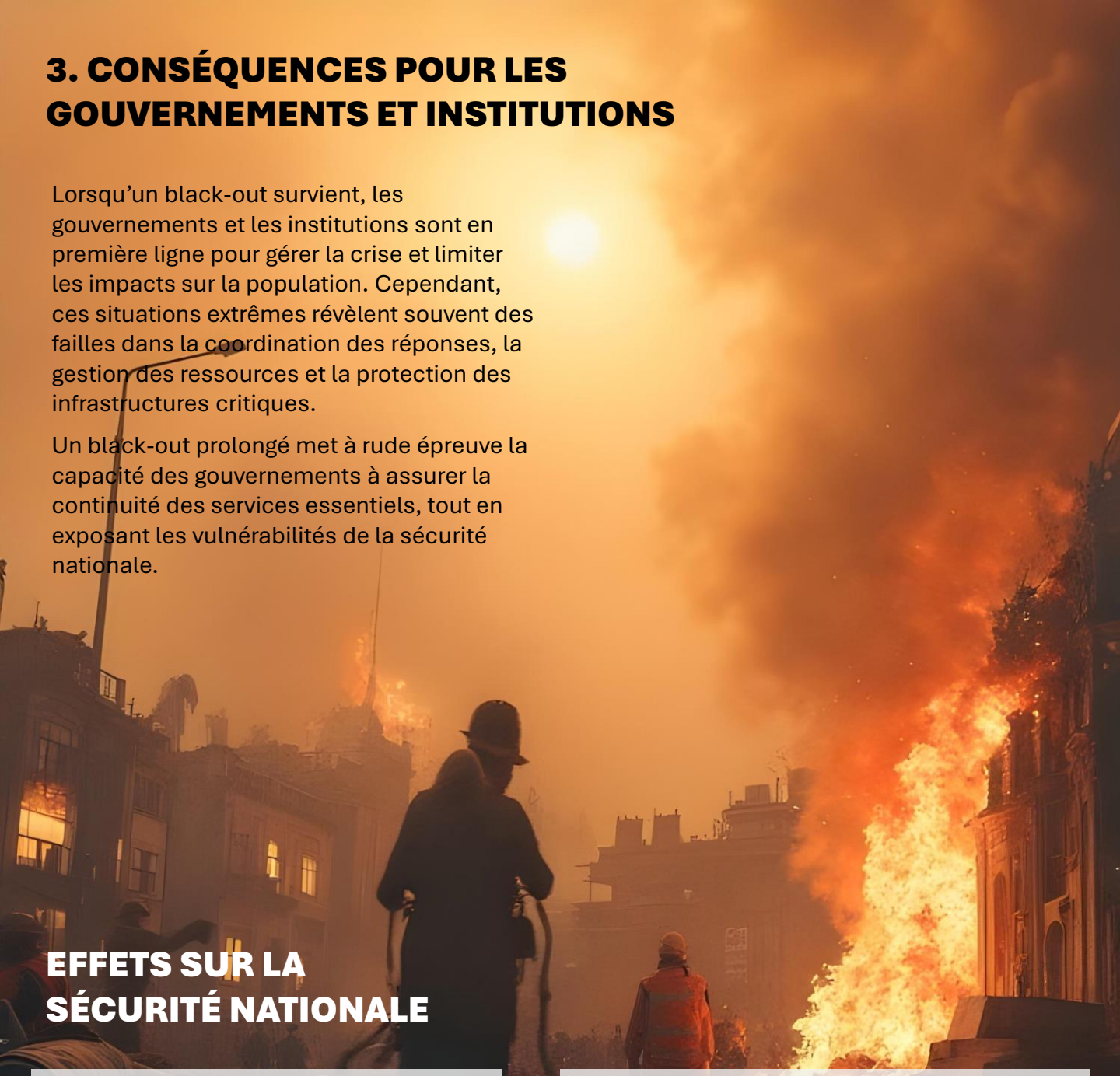
L’indisponibilité des réseaux de communication complique la gestion de crise.

Les autorités peinent à diffuser les consignes de sécurité à la population, ce qui peut intensifier la panique. Dans ces moments, les médias traditionnels, comme la radio, deviennent un outil essentiel de communication. Toutefois, leur efficacité dépend de la disponibilité de radios à batterie, souvent en quantité limitée dans les foyers.

3. CONSÉQUENCES POUR LES GOUVERNEMENTS ET INSTITUTIONS

Lorsqu'un black-out survient, les gouvernements et les institutions sont en première ligne pour gérer la crise et limiter les impacts sur la population. Cependant, ces situations extrêmes révèlent souvent des failles dans la coordination des réponses, la gestion des ressources et la protection des infrastructures critiques.

Un black-out prolongé met à rude épreuve la capacité des gouvernements à assurer la continuité des services essentiels, tout en exposant les vulnérabilités de la sécurité nationale.



EFFETS SUR LA SÉCURITÉ NATIONALE

Vulnérabilités exploitées par des acteurs malveillants

Un black-out prolongé expose les failles des systèmes nationaux, que des acteurs malveillants – terroristes ou États hostiles – peuvent exploiter.

Profitant du chaos généré par l'absence de communication et de coordination, ces acteurs peuvent mener des attaques supplémentaires ou aggraver la situation. Les cyberattaques synchronisées avec des pannes électriques peuvent maximiser l'impact destructeur, mettant à mal les infrastructures critiques.

Maintien de l'ordre public et prévention de l'anarchie

Pendant un black-out, maintenir l'ordre public est une priorité pour éviter l'anarchie. L'obscurité généralisée et l'absence de communication peuvent entraîner une montée de la criminalité, avec des pillages et des actes de vandalisme.

Les forces de sécurité doivent être rapidement déployées pour protéger les infrastructures critiques, maintenir la paix, et rassurer la population.

Cependant, des ressources limitées et une mauvaise coordination peuvent compliquer ces efforts, créant un environnement encore plus instable.

GESTION DE CRISE GOUVERNEMENTALE

Difficultés de coordination entre les différents niveaux de gouvernement

En période de black-out, la coordination entre les niveaux local, régional et national devient un véritable casse-tête.

Sans communication fluide, la prise de décision est freinée, rendant difficile l'exécution rapide des mesures de secours. Les désaccords ou les lenteurs administratives entre ces différentes instances peuvent aggraver la situation, laissant la population dans une situation critique sans réponse immédiate.

Mobilisation des ressources militaires et civiles

Face à un black-out majeur, les gouvernements doivent rapidement déployer à la fois des ressources civiles et militaires.

Les forces armées sont souvent appelées pour sécuriser les infrastructures critiques, distribuer des ressources vitales (eau, nourriture), et apporter un soutien logistique. Simultanément, les services de police, les pompiers, et les secours médicaux d'urgence sont mobilisés pour maintenir l'ordre public et gérer l'afflux de demandes d'assistance.

CONTINUITÉ DES SERVICES ESSENTIELS

Plans de continuité d’activité (PCA) et leurs limites

Bien que les gouvernements et institutions disposent de plans de continuité d'activité (PCA) pour garantir la disponibilité des services essentiels, un black-out prolongé révèle souvent leurs failles.

L’absence prolongée d’électricité et de communications complique la mise en œuvre de ces plans.

De plus, certaines infrastructures ne sont pas équipées pour résister à un black-out de longue durée : les générateurs de secours ont une autonomie limitée et ne suffisent pas à maintenir les services pendant des semaines.

Adaptation des infrastructures critiques

En situation de crise, les infrastructures critiques doivent s'adapter rapidement pour garantir un minimum de fonctionnement.

Cela inclut l’installation de systèmes de secours performants, tels que des générateurs, des réserves de carburant, et des solutions de redondance pour éviter les pannes critiques.

L’adaptation inclut également la mobilisation des ressources humaines pour pallier les défaillances technologiques, garantissant une présence humaine là où les systèmes automatisés ne fonctionnent plus.

4. IMPACTS SUR LES ENTREPRISES

Les entreprises sont particulièrement vulnérables face à un black-out, qu'il soit électrique ou informatique.

Lorsqu'une panne survient, elle perturbe non seulement la production et la logistique, mais expose également les entreprises à des pertes financières, des interruptions d'activité prolongées et des ruptures de communication avec leurs clients et partenaires.

La capacité d'une entreprise à réagir efficacement et à maintenir une continuité d'activité devient alors cruciale pour minimiser les dégâts.

INTERRUPTION DES CHAÎNES DE PRODUCTION ET DE DISTRIBUTION

Difficultés d'approvisionnement

En cas de black-out, les entreprises font face à des perturbations majeures dans leurs chaînes d'approvisionnement.

Les fournisseurs, eux-mêmes affectés par les coupures, ne peuvent souvent pas livrer les matières premières ou les produits dans les délais.

Cela désorganise l'ensemble de la chaîne de valeur, créant des retards et des interruptions dans la production, avec des conséquences en cascade sur les activités de l'entreprise.

Conséquences sur la logistique (pertes de marchandises, écarts de livraison)

La logistique est particulièrement vulnérable lors d'un black-out.

Les systèmes de gestion des stocks et de transport deviennent inopérants, compliquant la coordination des livraisons et le suivi des expéditions.

Les marchandises périssables sont en danger sans réfrigération, entraînant des pertes importantes.

Les écarts de livraison provoquent des pénuries, une insatisfaction des clients et affectent directement la réputation de l'entreprise.

IMPACTS ÉCONOMIQUES

Pertes financières et impacts sur la bourse

Les pertes financières dues à un black-out peuvent être considérables pour les entreprises, allant de l'interruption de leurs activités à la destruction de marchandises et aux coûts liés à la reprise.

Les secteurs comme la fabrication, la logistique et le commerce de détail sont particulièrement exposés.

De plus, l'incertitude générée par un black-out peut entraîner une volatilité accrue sur les marchés financiers, affectant négativement la valeur des actions et la valorisation des entreprises.

Relations avec les partenaires et clients

Un black-out peut fortement éroder la confiance des partenaires commerciaux et des clients.

Les retards de livraison, la perte de données, ou l'incapacité à honorer des engagements contractuels peuvent entraîner des ruptures de contrats ou des conflits.

Pour minimiser l'impact, les entreprises doivent maintenir une communication proactive avec leurs partenaires et clients, gérer les attentes et offrir des solutions d'atténuation pour préserver les relations commerciales à long terme.

REPRISE INFORMATIQUE ET CONTINUITÉ D'ACTIVITÉ

Plan de Reprise Informatique (PRI) et actions d'urgence

Face à un black-out, les entreprises doivent au besoin activer leur Plan de Reprise Informatique (PRI) pour restaurer leurs systèmes critiques qui ont été piratés.

Cela inclut l'utilisation des sauvegardes, la mobilisation des équipes techniques et la restauration des services prioritaires.

Cependant, l'efficacité du PRI dépend de la capacité de l'entreprise à accéder aux ressources d'urgence, un défi encore plus grand lors d'un black-out prolongé, où l'accès aux équipements est souvent limité.

Différences entre black-out partiel et total

La nature du black-out influence directement la reprise d'activité.

Dans un black-out partiel, certaines infrastructures peuvent rester fonctionnelles, facilitant une reprise progressive.

En revanche, un black-out total complique grandement la situation : l'absence complète de ressources électriques et de connectivité nécessite une mobilisation accrue et une coordination rigoureuse pour restaurer les activités de manière ordonnée.

5. CONSÉQUENCES SUR LA POPULATION

Un black-out, ne touche pas seulement les infrastructures ou les entreprises. Il bouleverse également le quotidien des populations, avec des répercussions immédiates sur l'accès aux ressources essentielles, la santé et la sécurité.

Dans un contexte où l'incertitude et la panique peuvent rapidement s'installer, certaines personnes, notamment les plus vulnérables, sont particulièrement exposées.

Cependant, ces périodes de crise révèlent aussi des comportements adaptatifs et des élans de solidarité qui témoignent de la résilience collective.

VIE QUOTIDIENNE PERTURBÉE

Accès limité à l'eau, à la nourriture et aux biens de première nécessité

Lors d'un black-out, l'accès aux ressources essentielles devient rapidement problématique.

Les infrastructures de distribution d'eau potable, fortement dépendantes de l'électricité, peuvent être perturbées, limitant l'accès à une eau saine pour la consommation.

Les supermarchés, incapables de fonctionner sans électricité, ferment leurs portes, compliquant l'approvisionnement en nourriture.

De plus, la rupture des chaînes logistiques peut entraîner des pénuries de biens de première nécessité, privant ainsi de nombreuses personnes des ressources indispensables à leur survie.

Gestion des urgences de santé à domicile

Les personnes dépendant d'équipements médicaux à domicile, tels que les concentrateurs d'oxygène ou les ventilateurs, sont particulièrement vulnérables lors d'un black-out.

Sans électricité, ces dispositifs deviennent inutilisables, mettant la vie des patients en danger.

L'accès limité aux services de secours et la saturation des lignes d'urgence aggravent la gestion des crises médicales à domicile, nécessitant des solutions alternatives et une entraide communautaire pour combler les manques.

PEUR ET PANIQUE

L’absence d’informations claires et l’incertitude quant à la durée d’un black-out peuvent rapidement déclencher un sentiment de panique au sein de la population.

La peur de manquer de ressources essentielles, combinée à l'isolement provoqué par l'indisponibilité des réseaux de communication, peut mener à des comportements irrationnels tels que des achats de panique ou des mouvements de foule désorganisés.

Ces réactions exacerbent la situation et compliquent encore davantage la gestion de la crise.

VULNÉRABILITÉ ACCRUE DES POPULATIONS FRAGILES

Les populations les plus fragiles, telles que les personnes âgées, les malades chroniques et les communautés défavorisées, sont particulièrement exposées lors d’un black-out.

Les personnes âgées peuvent avoir des difficultés à se déplacer pour obtenir des ressources de base, tandis que les malades chroniques subissent l'interruption de leurs soins réguliers.

Quant aux populations défavorisées, elles sont souvent les moins préparées à faire face à une crise prolongée, manquant de réserves de nourriture, d'eau ou d’argent pour subvenir à leurs besoins.

Sans accès aux services de soutien habituels, ces groupes voient leur santé et leur sécurité gravement menacées.

COMPORTEMENTS ADAPTATIFS ET SOLIDARITÉ

Malgré la panique initiale, les périodes de black-out révèlent aussi des élans de solidarité et d'entraide. Heureusement ...

Les communautés s'organisent souvent pour partager les ressources disponibles, soutenir les personnes vulnérables et apporter de l'aide à ceux qui en ont besoin.

Des réseaux d'entraide spontanés voient le jour pour distribuer des vivres, échanger des informations, ou organiser une surveillance collective afin de maintenir la sécurité.

Ces dynamiques positives montrent l'importance cruciale de la résilience communautaire dans la gestion des crises.

6. LE BLACK-OUT COMME OPPORTUNITÉ DE RÉSILIENCE

Un black-out, bien qu'il soit une crise majeure, peut aussi être une occasion de transformation.

Chaque coupure massive d'électricité ou de systèmes informatiques révèle des faiblesses, mais offre également des enseignements précieux pour renforcer la résilience collective et améliorer la préparation future.

Plutôt que de subir ces événements, les communautés, les entreprises et les gouvernements peuvent les utiliser comme des opportunités pour s'adapter, moderniser leurs infrastructures et renforcer leurs capacités à faire face aux crises.

APPRENTISSAGE COLLECTIF ET ADAPTABILITÉ

Initiatives communautaires pour renforcer la résilience

Bien qu'un black-out soit souvent perçu comme un événement traumatisant, il peut également représenter une opportunité pour renforcer la résilience collective.

Les communautés peuvent tirer parti de ces crises pour mettre en place des initiatives locales visant à partager les meilleures pratiques et à améliorer la préparation face aux futures crises.

Des exercices de simulation de black-out, par exemple, peuvent être organisés pour éduquer les habitants sur la gestion d'une coupure prolongée, tout en favorisant la solidarité et une répartition efficace des ressources.

Rôle des organisations dans la diffusion de bonnes pratiques

Les organisations, qu'elles soient publiques ou privées, jouent un rôle clé dans la diffusion de bonnes pratiques pour faire face à un black-out.

Elles peuvent sensibiliser les populations sur les gestes à adopter, former leurs employés à la gestion des urgences, et s'assurer que des plans de continuité robustes sont en place.

Le partage des enseignements tirés des crises passées renforce l'adaptabilité des communautés et des entreprises, contribuant à un système plus résilient face aux perturbations futures.

RENFORCEMENT DES SYSTÈMES CRITIQUES

Leçons tirées des crises passées

Chaque black-out laisse des enseignements précieux, permettant d'améliorer la résilience des infrastructures critiques.

En analysant les défaillances observées lors de précédentes crises, il est possible d'identifier les points faibles et de mettre en place des mesures correctives.

Par exemple, les blackouts passés ont mis en lumière l'importance cruciale de la redondance dans les systèmes de communication et l'amélioration des systèmes de secours pour garantir une continuité de service, même en cas de coupure prolongée.

Modernisation des infrastructures pour une plus grande tolérance aux pannes

Pour renforcer la résilience face aux blackouts, la modernisation des infrastructures est indispensable.

Cela inclut l'intégration de technologies intelligentes capables de détecter et de réagir plus rapidement aux pannes dans les réseaux électriques, ainsi que la diversification des sources d'énergie (solaire, éolienne, etc.) pour limiter la dépendance à un seul type de production.

Le développement de micro-réseaux autonomes peut également permettre de maintenir l'alimentation des infrastructures critiques, même en cas de coupure généralisée.

7. COMMENT SE PRÉPARER À UN BLACK-OUT

Un black-out peut survenir à tout moment, et ses conséquences sont souvent dévastatrices.

Cependant, une préparation adéquate peut considérablement atténuer les impacts d'une telle crise, que ce soit au niveau des infrastructures critiques, des entreprises, des gouvernements ou des citoyens.

La clé réside dans l'anticipation : renforcer les systèmes, tester les plans d'urgence et assurer la coordination entre les différents acteurs.

PRÉPARATION DES INFRASTRUCTURES CRITIQUES

Renforcement des systèmes de secours

Les infrastructures critiques, telles que les hôpitaux, les centrales électriques, et les systèmes de communication, doivent être équipées de systèmes de secours robustes et redondants.

Cela inclut l'installation de générateurs de secours, la mise en place de micro-réseaux autonomes, ainsi que l'amélioration des capacités de stockage d'énergie.

Il est également essentiel de former le personnel à l'utilisation de ces systèmes en situation d'urgence pour garantir une réaction rapide et efficace.

Tests réguliers et maintenance

Des tests réguliers des infrastructures sont indispensables pour s'assurer du bon fonctionnement des équipements de secours et des plans de continuité.

La maintenance préventive permet d'éviter des défaillances imprévues en cas de black-out prolongé, assurant ainsi la continuité des services essentiels.

PRÉPARATION DES ENTREPRISES

Plans de Continuité d'Activité (PCA)

Chaque entreprise doit élaborer un Plan de Continuité d'Activité (PCA) pour garantir la poursuite de ses opérations pendant un black-out.

Cela inclut l'identification des processus critiques, la mise en place de solutions alternatives, et la formation des employés à travailler dans des conditions dégradées.

Les PCA doivent être régulièrement testés pour vérifier leur efficacité face à des scénarios réels.

Stockage et redondance des données

La sauvegarde régulière des données critiques est indispensable, avec idéalement plusieurs copies sur différents sites géographiques.

L'utilisation du cloud hybride et des solutions de Disaster Recovery as a Service (DRaaS) permet de garantir l'accès aux informations vitales, même en cas de panne des infrastructures principales.

PRÉPARATION DES GOUVERNEMENTS ET INSTITUTIONS PUBLIQUES

Plans de gestion de crise

Les gouvernements doivent disposer de plans de gestion de crise spécifiques aux black-out, incluant la coordination des agences gouvernementales, la mobilisation des ressources (militaires et civiles) et la communication avec le public.

Des exercices réguliers sont essentiels pour tester la réactivité des différents acteurs et affiner les procédures.

Communication et information du public

La communication est cruciale pour éviter la panique et maintenir l'ordre public lors d'un black-out.

Les gouvernements doivent prévoir des moyens de communication alternatifs, comme les radios à ondes courtes, pour diffuser des informations en temps réel.

Des campagnes de sensibilisation doivent également préparer les citoyens à adopter les comportements appropriés en cas de crise.

PRÉPARATION DES CITOYENS

Constitution de stocks de survie

Chaque citoyen doit se préparer à un black-out prolongé en constituant des stocks de nourriture non périssable, d'eau, de médicaments et de batteries.

Une autonomie d'au moins une semaine est recommandée pour faire face à une interruption prolongée des services.

Apprentissage des gestes de premiers secours et d'autonomie

En cas de black-out, les services de secours peuvent être saturés.

Il est donc crucial que les citoyens soient formés aux gestes de premiers secours et à des compétences pratiques comme la filtration de l'eau ou la conservation des aliments.

Participation aux initiatives communautaires

La solidarité est un élément clé de la résilience lors d'un black-out.

Les citoyens sont encouragés à participer aux initiatives communautaires, telles que les réseaux de voisins solidaires, afin de partager les ressources et d'offrir une entraide mutuelle en cas de crise prolongée.

En parcourant ce dossier, nous avons mis en lumière les multiples risques que les black-out électriques et informatiques font peser sur nos sociétés, qu'ils soient provoqués par des causes naturelles, humaines ou cybernétiques.

Les impacts sur les infrastructures critiques, les gouvernements, les entreprises et, bien sûr, la population sont énormes, et chaque secteur a ses vulnérabilités spécifiques.

Ce qui ressort avant tout des exemples passés, c'est l'importance de renforcer notre résilience collective et de moderniser nos systèmes pour mieux faire face à ces crises inévitables.

Se préparer à un black-out ne doit plus être perçu comme une option, mais comme une nécessité.

Que ce soit en renforçant les systèmes critiques, en sensibilisant nos citoyens, ou en mettant en place des plans de continuité d'activité robustes, c'est cette préparation qui nous permettra de limiter les impacts dévastateurs.

Un black-out prolongé peut provoquer des perturbations profondes, mais avec les bonnes mesures en place, nous pouvons surmonter ces épreuves et en ressortir plus forts.

J'aimerais que vous, en tant que lecteur, preniez ce moment pour réfléchir à votre propre rôle dans cette préparation.

Les gouvernements ont la responsabilité de garantir la résilience des infrastructures critiques et de coordonner efficacement la gestion de crise.

Les entreprises doivent, de leur côté, s'assurer qu'elles ont un plan de continuité testé et prêt à être déployé.

Mais vous, individuellement, êtes-vous prêt ?

- Avez-vous pensé à ces ressources essentielles qui pourraient faire toute la différence en cas de coupure prolongée ?
- Êtes-vous connecté à vos voisins, à votre communauté, pour faire face ensemble ?

Nous avons tous un rôle à jouer, et c'est dans l'action collective que réside notre vraie force.

PRÉPAREZ-VOUS MAINTENANT, POUR SURVIVRE AU BLACK-OUT...

Alexandre Fournier

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

www.crise-resilience.com

Pannes électrique majeur

Année	Pays/Région	Personnes affectées
1965	États-Unis, Canada	30 millions
1977	New York, États-Unis	9 millions
1978	France	3/4 du pays
1989	Québec, Canada	6 millions
1998	Québec, Canada	4 millions
1999	France	3,6 millions
2003	Nord-Est des États-Unis, Canada	55 millions
2003	Italie	56 millions
2006	Europe	15 millions
2009	Brésil, Paraguay	87 millions
2011	Japon	4 millions
2012	Inde	670 millions
2019	Argentine, Uruguay, Paraguay	48 millions
2021	Texas, États-Unis	4,5 millions
2023	Tunisie	Majorité du pays

Informations complémentaires

Ice Storm of 1998
https://www.thecanadianencyclopedia.ca/en/article/ice-storm-1998

Northeast blackout of 2003
https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

Power grid cyberattack in Ukraine (2015)
https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)

The Grid: The Fraying Wires Between Americans and Our Energy
https://www.amazon.com/Grid-Fraying-Between-Americans-Energy/dp/1608196100

Evaluation of grid operational resilience stressed by energy transition and by climate change: new metrics (SIRI) and countermeasures
https://www.cigre.org/article/GB/evaluation-of-grid-operational-resilience-stressed-by-energy-transition-and-by-climate-change-new-metrics-siri-and-countermeasures

Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath
https://www.goodreads.com/book/show/37806696-lights-out%5B1

L'ESSENTIEL - GUIDE DE SURVIE LORS D'UN BLACK-OUT

AVANT LE BLACKOUT : PRÉPAREZ-VOUS

Un blackout peut arriver à tout moment. Se préparer à l'avance est essentiel pour minimiser l'impact sur votre sécurité et votre confort.

1.Stockez de l'eau et de la nourriture : Prévoyez au moins trois jours de nourriture non périssable et de l'eau potable (environ 4 litres par jour et par personne). Les aliments en conserve et les barres énergétiques sont pratiques.

2.Créez un kit de survie : Assemblez une lampe de poche, des bougies, des allumettes ou un briquet, des batteries de rechange, une radio à manivelle, et un chargeur de téléphone solaire ou portable.

3.Prévoyez une source de chaleur : En hiver, ayez des couvertures chaudes, des sacs de couchage, et des vêtements en couches. Une source de chauffage indépendante (comme un poêle à bois) peut être un vrai plus.

4.Médicaments et premiers secours : Assurez-vous de posséder un stock de vos médicaments essentiels et une trousse de premiers secours complète.

5.Planifiez les communications : Notez les numéros d'urgence et prévenez vos proches de vos plans en cas de coupure. Ayez des talkies-walkies ou une radio CB pour rester en contact.

PENDANT LE BLACKOUT : RESTEZ EN SÉCURITÉ

Pendant un blackout, le plus important est de rester calme et d'éviter les situations dangereuses.

1.Gérez la lumière et la chaleur : Utilisez des lampes de poche plutôt que des bougies pour minimiser les risques d'incendie. Limitez les déplacements inutiles pour conserver la chaleur.

2.Conservez la nourriture : Gardez le réfrigérateur et le congélateur fermés autant que possible pour maintenir la fraîcheur des aliments. Les congélateurs peuvent garder les aliments congelés jusqu'à 48 heures si les portes restent fermées.

3.Hydratez-vous et évitez l'effort inutile : Conservez votre énergie et évitez de vous fatiguer inutilement. Buvez régulièrement de l'eau.

4.Écoutez les consignes des autorités : Utilisez votre radio à piles pour obtenir les mises à jour des autorités locales sur la durée prévue de la coupure et les mesures à prendre.

5.Utilisez prudemment les sources de chaleur : Si vous utilisez un poêle ou un générateur, assurez-vous qu'ils sont correctement ventilés pour éviter les intoxications au monoxyde de carbone.

APRÈS LE BLACKOUT : REPRENEZ LE CONTRÔLE

Lorsque l'électricité est restaurée, il est important de faire une vérification de votre environnement avant de revenir à la normale.

1.Vérifiez les appareils : Débranchez les appareils sensibles pour éviter les surtensions à la reprise du courant. Inspectez vos équipements pour vous assurer qu'ils fonctionnent correctement.

2.Contrôlez la qualité de la nourriture : Jetez les aliments périssables qui ont été exposés à des températures supérieures à 4°C pendant plus de quatre heures.

3.Réapprovisionnez votre kit : Remplacez les éléments de votre kit de survie que vous avez utilisés, comme les batteries, les bougies, et l'eau potable.

4.Apprenez de l'expérience : Prenez le temps de faire une réflexion sur ce qui a bien fonctionné et ce qui pourrait être amélioré. Cela vous aidera à être mieux préparé pour la prochaine fois.

5.Rassurez vos proches : Informez vos amis et votre famille de votre situation actuelle et assurez-vous que tout le monde est en sécurité.

CRISE & RÉSILIENCE C'EST... AUSSI

Une chaîne YouTube avec...

Des conférences et formations gratuites

Des interviews d'experts :

Des réponses à vos questions :

https://www.youtube.com/criseetresilience

Une page LinkedIn avec...

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

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

Des formations ACADEMIE CRISE & RÉSILIENCE sur...

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

https://www.academiecriseetresilience.com/

ABONNEZ-VOUS Gratuitement

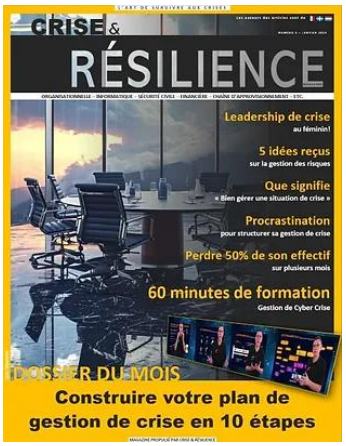
TRIMESTRIEL – JANVIER – AVRIL – JUILLET – OCTOBRE

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

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 un 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!



Abonnez-vous sur www.criseetresilience-magazine.com

La chaîne YouTube Crise & Résilience

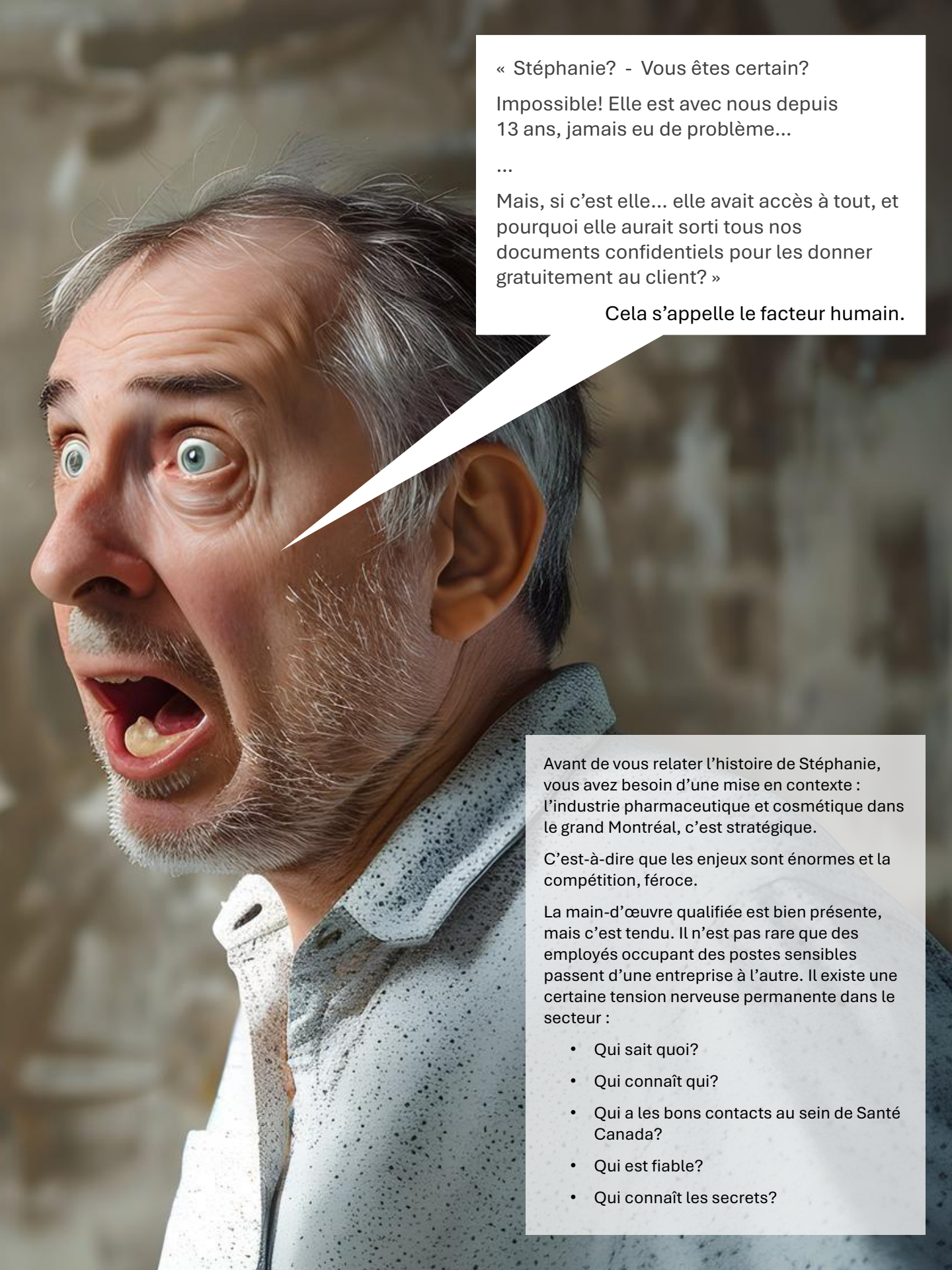
Des conférences et formations gratuites

Des interviews d'experts :

Un employé déloyal et le bris de confiance, ça fait très mal!

C’est à la fois la pire situation et la plus fréquente. Cela vous est forcément déjà arrivé et vous y pensez encore. Alors, sortons du cauchemar.

Par Philippe Chevalier
Cofondateur de Sarx
Agence de détectives d’affaires

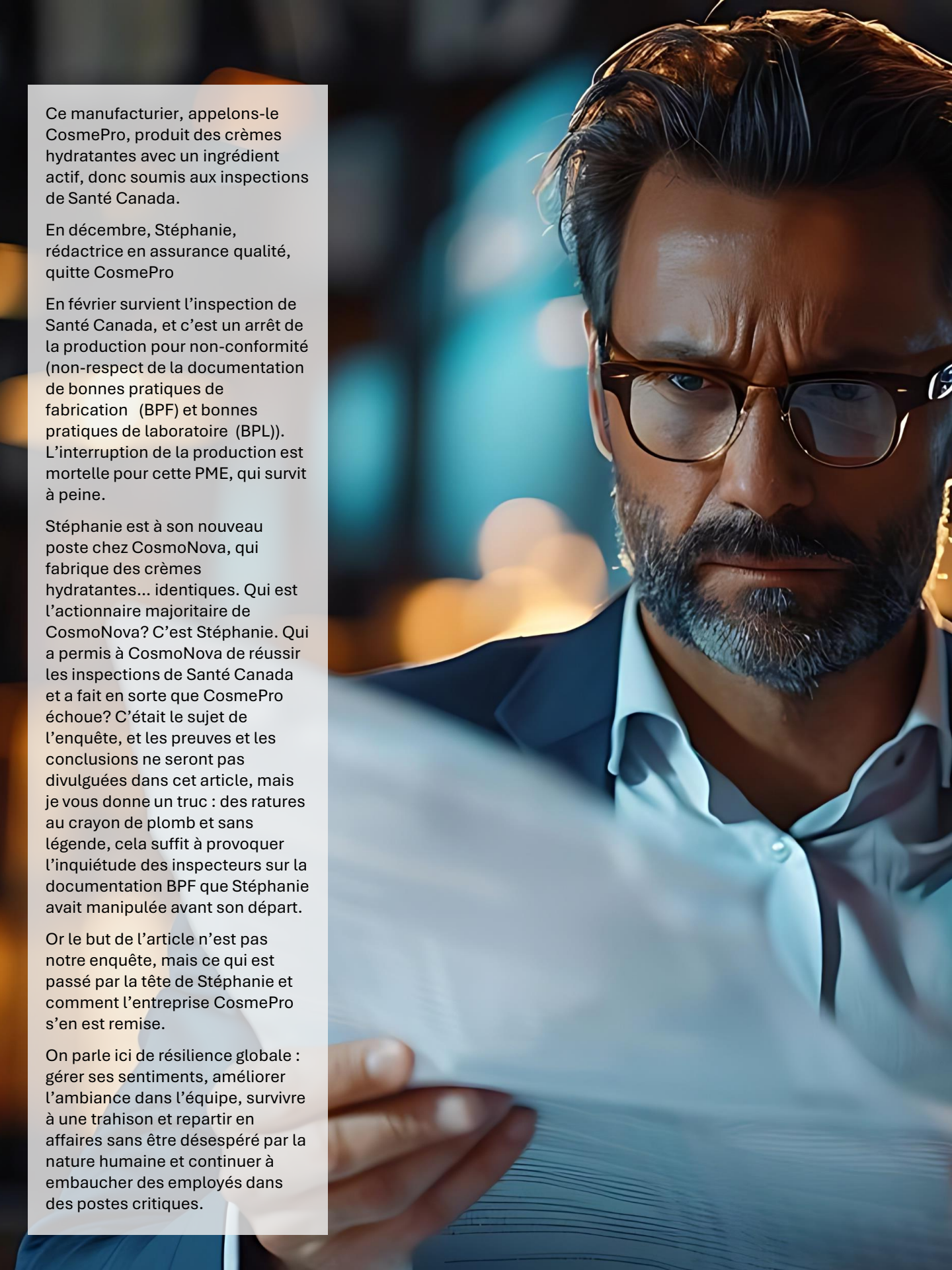


Avant de vous relater l'histoire de Stéphanie, vous avez besoin d'une mise en contexte : l'industrie pharmaceutique et cosmétique dans le grand Montréal, c'est stratégique.

C'est-à-dire que les enjeux sont énormes et la compétition, féroce.

La main-d'œuvre qualifiée est bien présente, mais c'est tendu. Il n'est pas rare que des employés occupant des postes sensibles passent d'une entreprise à l'autre. Il existe une certaine tension nerveuse permanente dans le secteur :

- Qui sait quoi?
- Qui connaît qui?
- Qui a les bons contacts au sein de Santé Canada?
- Qui est fiable?
- Qui connaît les secrets?



Ce manufacturier, appelons-le CosmePro, produit des crèmes hydratantes avec un ingrédient actif, donc soumis aux inspections de Santé Canada.

En décembre, Stéphanie, rédactrice en assurance qualité, quitte CosmePro

En février survient l'inspection de Santé Canada, et c'est un arrêt de la production pour non-conformité (non-respect de la documentation de bonnes pratiques de fabrication (BPF) et bonnes pratiques de laboratoire (BPL)). L'interruption de la production est mortelle pour cette PME, qui survit à peine.

Stéphanie est à son nouveau poste chez CosmoNova, qui fabrique des crèmes hydratantes… identiques. Qui est l'actionnaire majoritaire de CosmoNova? C'est Stéphanie. Qui a permis à CosmoNova de réussir les inspections de Santé Canada et a fait en sorte que CosmePro échoue? C'était le sujet de l'enquête, et les preuves et les conclusions ne seront pas divulguées dans cet article, mais je vous donne un truc : des ratures au crayon de plomb et sans légende, cela suffit à provoquer l'inquiétude des inspecteurs sur la documentation BPF que Stéphanie avait manipulée avant son départ.

Or le but de l'article n'est pas notre enquête, mais ce qui est passé par la tête de Stéphanie et comment l'entreprise CosmePro s'en est remise.

On parle ici de résilience globale : gérer ses sentiments, améliorer l'ambiance dans l'équipe, survivre à une trahison et repartir en affaires sans être désespéré par la nature humaine et continuer à embaucher des employés dans des postes critiques.

Pourquoi un employé devient déloyal?

Les êtres humains ont des réactions variées face aux événements de la vie. Certains sont résilients et antifragiles, d'autres deviennent aigris et en colère :

- **Bouleversement dans la vie personnelle**, maladie (chez soi-même ou chez un proche), séparation, besoin de revanche, besoins financiers urgents : tout ce qui paraissait normal, éthique, juste et moral devient futile et méprisable; c'est le moment de survivre et de penser à soi.
- **Influence extérieure** : nouvelle vie sentimentale, nouveaux besoins financiers, fascination subite pour la réussite financière et entrepreneuriale, perte de repères.
- **Frustration** : manque de reconnaissance, compétition interne, conflits dans l'équipe, désir de revanche, fatigue d'être critiqué par le patron parce qu'on ralentit la production pour des questions réglementaires (c'est ce que vivent souvent les responsables en assurance qualité).
- **Malhonnêteté naturelle, opportunisme brutal** : bien sûr, cela existe aussi, de même qu'existe une idéologie qui prétend qu'en affaires, tous les coups sont permis.

Le cas de Stéphanie est quelque part dans la liste ci-dessus.

Est-ce que l'entreprise aurait pu voir venir la trahison?

Pas dans toutes les causes évoquées plus haut, mais, pour plusieurs d'entre elles, c'était possible avec un peu d'attention pour les signaux faibles.

Les enquêteurs internes des grandes entreprises et nous aussi, comme enquêteurs externes, nous menons parfois ces exercices de veille tant que nous ne brisons pas l'expectative de vie privée.

Comment une entreprise peut-elle survivre?

En combattant et en combattant vite et sans pitié.

N'allez pas croire que l'absence de clauses de non-concurrence vous empêche de vous battre (pas si fréquentes, ces clauses, en dehors des vendeurs et des représentants, et de moins en moins acceptées par les candidats).

Les préjudices, le sabotage, la déloyauté peuvent être démontrés. Bref, il faut se battre!

Et CosmePro s'est battue, a contre-attaqué, a convaincu Santé Canada, a démontré et a prouvé la déloyauté et, surtout, le sabotage.

Le conflit fut résolu par la négociation, car aucune des deux entreprises n'a voulu se rendre devant les tribunaux. CosmePro a été plus que résiliente, elle a réagi et elle est devenue antifragile.

J'ai non seulement changé le nom des entreprises, mais mixé trois dossiers différents pour faire un seul article et protéger la confidentialité. Toutefois, si vous connaissez un peu le milieu de la production pharmaceutique ou cosmétique, vous savez que tous les éléments sont authentiques.

Vous soupçonnez qu'un employé ou un associé soit déloyal ?

1. Pas de déni, la déloyauté existe en affaires.
2. Montez un dossier immédiatement, rassemblez des preuves sans crainte de vous tromper. Si vous vous trompez, vous détruirez le dossier, mais si vous ne vous trompez pas, vous feriez mieux d'être équipé.
3. Appliquez le proverbe La confiance n'empêche pas le contrôle. Vous avez le droit de contrôler ce qui est contrôlable, cela ne doit insulter personne.
4. Les déloyautés ne viennent pas subitement. Savez-vous ce que sont les signaux faibles?
5. Mettez autant de soin à une entrevue de fin d'emploi qu'à une entrevue de recrutement. Demandez-vous dans quel état l'employé ou l'associé vous quitte (et... avec quelles informations).
6. Ne menez pas d'enquête par vous-même en dehors de votre entreprise. Les enquêteurs privés spécialisés en entreprise ont les moyens, les outils, et connaissent le contexte légal.
7. N'espionnez personne, ça constitue un délit. Laissez la surveillance et l'enquête aux enquêteurs.
8. Restez déterminé, faites intervenir rapidement un avocat, au moins pour vous guider.
9. Les clauses de non-concurrence sont contournables, mais la déloyauté se prouve avec ou sans clause. C'est un concept différent, alors ne craignez pas de foncer contre l'adversaire.
10. Mais... parfois, il faut négocier. Le combat judiciaire n'est pas toujours la meilleure option. Vous ne pourrez cependant négocier en position de force que si vous détenez des preuves.

Si vous survivez à une déloyauté, ce sera de la super-résilience, car votre entreprise aura surmonté la plus douloureuse des épreuves.

Mais une chose est certaine, et cela peut vous surprendre comme ultime recommandation : continuez quand même à faire confiance.

La résilience après une catastrophe climatique, une pandémie, un changement d'algorithme sur Google ou toute autre catastrophe est une chose, mais la résilience après une déloyauté (employé ou associé) est une tout autre affaire.

Vous ne vous battrez pas contre des fatalités, mais contre des personnes, et il faut l'accepter avec détermination.

Les justes finissent toujours par gagner (surtout si on les aide un peu).

Philippe Chevalier

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

Cybercriminalité et compliance : quels défis pour le secteur financier?

À l'heure où les modes opératoires des criminels dans le cyberespace deviennent de plus en plus sophistiqués et ciblent stratégiquement des secteurs économiques variés, les professionnels de la lutte contre le blanchiment et le financement du terrorisme (LCB-FT) s'exposent à des enjeux multifactoriels qui les invitent à renforcer leur analyse des risques.

par Vanessa Lahmy

Consultante Compliance et Gestion des risques
Formatrice Droit et Sécurité financière

Spécialiste Lutte contre la criminalité financière, financement du terrorisme et contournement des sanctions internationales

À l'ère de la révolution numérique portée par l'intelligence artificielle, la dynamique des réseaux cybercriminels augmente en puissance.

La cybercriminalité étant désormais un vecteur répandu de blanchiment d'argent et de financement d'activités terroristes, les professionnels de la compliance font face à de nombreux défis pour prévenir et détecter ces risques.

Typologie des risques de cyberblanchiment et de cyberterrorisme

En tant qu'assujettis aux réglementations européennes de lutte contre le blanchiment d'argent et le financement d'activités terroristes, les professionnels du secteur financier sont soumis à un devoir de vigilance qui consiste principalement à mettre en œuvre des procédures et des contrôles internes visant à prévenir tout risque protéiforme de criminalité.

À l'heure où le cyberespace est dévoyé à des fins de revendication idéologique, politique et économique, devenant ainsi *« une arme de guerre à part entière(1) »*, les professionnels de la compliance doivent porter une attention particulière et incontournable à la cybercriminalité. En effet, si *« le crime n'abandonne jamais les secteurs traditionnels [...] il s'intéresse à la technologie pour développer ses capacités et son "offre de services" [...] de blanchiment »*, de sorte que le crime numérique vient désormais s'ajouter au crime traditionnel(2) . Il est d'ailleurs significatif de noter que les cyberfraudes représentent au total un chiffre d'affaires estimé à 8 000 milliards de dollars, érigeant ainsi l'industrie du cybercrime au rang de troisième économie mondiale(3).

Parmi les modalités classiques de propagation d'idéologies terroristes, deux types de cyberattaques majeurs s'appuient sur les techniques du Net : le ransomware (rançongiciel), qui consiste à pirater des données informatiques moyennant une demande de rançon, et le phishing (hameçonnage), une technique frauduleuse consistant à extorquer des coordonnées bancaires ou des identifiants de connexion puis des fonds(4) .

Les cyberfraudes représentent au total un chiffre d'affaires estimé à 8 000 milliards de dollars

La cybercriminalité au moyen des nouvelles technologies de l'information, au premier rang desquelles se trouve la blockchain, est par ailleurs en pleine expansion. Le stockage et l'échange décentralisés de données permettent, à grande échelle, le blanchiment lié par exemple au trafic de stupéfiants, par le biais du dark Web ou encore des organisations criminelles. Les professionnels du secteur bancaire devront à cet effet être particulièrement attentifs aux possibilités de paiement en ligne par cartes rechargeables en cryptomonnaie.

Détecter les risques de cybercriminalité dans le cadre de la relation d'affaires

L'une des procédures de prévention des risques consiste à effectuer une revue KYC (know your customer), dont l'étape fondamentale réside dans l'identification et la vérification de l'identité du client.

Or, s'agissant d'une opération effectuée via la blockchain, le professionnel de la compliance se trouve confronté à un défi majeur : le quasi anonymat que garantit ce mode de financement décentralisé, puisque les fonds transitent par des comptes où seules les adresses bitcoin peuvent être identifiées, et non l'identité du détenteur.

Comment, dès lors, assurer un suivi conforme des transactions sans pouvoir clairement identifier les individus qui en sont à l'origine? L'opacité des transactions permise par la blockchain n'est-elle pas au contraire aux antipodes du devoir de vigilance? Comme l'a souligné à juste titre un expert en criminologie, *« les lois actuelles, qui ciblent les émetteurs de monnaie, ne sont pas adaptées à la régulation du bitcoin(5) »*.

Par ailleurs, s'il faut saluer le renforcement de l'identification sécurisée par signature électronique qu'a permis le règlement européen eIDAS 2 depuis le 20 mai dernier, l'usage de l'intelligence artificielle générative, lui, est à redouter. Nombreuses sont les possibilités de falsification de l'identité par l'image, l'audio ou le texte. Les deepfakes permettent en ce sens les faux ordres de virement, la communication de théories complotistes ou encore des atteintes à l'identité numérique(6).

Enfin, fait plus tabou mais néanmoins bien réel : la corruption en interne de professionnels du secteur financier par les cybercriminels eux-mêmes. Mais quand bien même la tentative échouerait, l'industrie du cybercrime ne serait pas pour autant amoindrie. Car de l'aveu de certains criminels, *« [...] hackeur n'est pas seulement un job, c'est aussi une passion(7) »*.

Là réside peut-être la plus grande préoccupation, car c'est bien connu : rien ne peut arrêter un passionné dans son engouement, même utilisé à mauvais escient.

Si des techniques déjà éprouvées de lutte anti-blanchiment et contre – terrorisme permettent aux professionnels de la compliance de piloter efficacement la gestion des risques de criminalité financière, le cyber espace détourné et l'essor des nouvelles technologies insuffisamment régulées restent des sources de défis non négligeables au regard de la protection de données sensibles, de la vérification numérique de l'identité et de la surveillance des transactions numériques.

Car les hackers changent de profils avec agilité, et leurs visages sont multiples.

Autant de points de vigilance qui nécessitent avant tout une intelligence humaine: allier compétences techniques et facultés intuitives.

Vanessa Lahmy

VL CONSULTING est un cabinet de conseil spécialisé dans l'analyse et la gestion des risques opérationnels de criminalité financière. Il facilite la mise en place de contrôles internes pour les professionnels et les sensibilise à la LCB-FT en France et à l'international.

Email: v.lahmy@consultant.com

4 conseils pratiques pour faire face aux risques de cybercriminalité

- Sortir de sa zone de confort professionnelle est indispensable. Restez constamment en alerte sur l'actualité et l'évolution des risques dans divers secteurs d'activités, aussi bien public que privé, à l'échelle nationale et internationale. N'hésitez pas aussi à échanger les bonnes pratiques avec vos pairs, à vous documenter et, surtout, à élargir vos cercles de réseaux afin de capter des informations utiles à mettre en application dans votre sphère professionnelle.
- Faites usage de votre leadership en incitant vos collègues à s'impliquer davantage dans l'hygiène numérique et en les encourageant à accorder de l'importance à la sensibilisation.
- Adoptez une grille de lecture transversale et globale des risques. Une collaboration étroite entre les différents départements de votre société, notamment en technologies de l'information et en compliance, est indispensable pour faire remonter les problèmes rencontrés et réfléchir à des solutions optimales de façon collaborative.
- Contribuez à mettre en place des infrastructures suffisamment robustes en interne en allant au-delà des prérequis et des recommandations de base telles que le dispositif de protection des données sensibles.

Références :

1. Clapaud, A. (2023). Le Cybercrime, une industrie à part entière. Le guide 2023-2024 : cybersécurité (hors-série, p. 32). Solutions Numériques.
2. Bauer, A. (2024, mars). La cyberguerre n'a pas encore commencé. Et nous n'y sommes pas prêts. *Solutions numériques & cybersécurité*, (1), 44.
3. Morgan, S. (2022). *2022 Official Cybercrime Report*. eSentire et Cybersecurity Ventures.
4. Akasbi, M. (2023, décembre). IA : outil de fraude et de lutte contre la fraude. *Revue de l'Union européenne*, (673), 620.
5. Fortin, F. (2024, juin-septembre). La cybercriminalité et ses enjeux. *Questions internationales*, (125-126), 64.
6. Ministère de l'Intérieur et des Outre-mer. (2024). *Rapport annuel sur la cybercriminalité 2024*. France.
7. Monnet, B. (2022, mai-juillet). La faille, arme du cybercriminel. *Les mafias : quand le crime organisé menace le monde (Le Monde Hors-série)*, 49.

Audit DORA : vers une nouvelle ère de résilience digitale

Face à une menace cyber croissante, le secteur bancaire doit renforcer sa résilience digitale.

Découvrez comment DORA redéfinit les standards de sécurité et la gestion des tiers et des fournisseurs cloud, (Services infonuagiques) et pourquoi un audit rigoureux est essentiel pour protéger les institutions financières des risques opérationnels et pour garantir leur stabilité future.

Par Teddy Ramanakasina

Directeur associé – sécurité de l'information

Audit technologique, responsable en cybersécurité, conseiller en gestion des risques, analyse de données, risques liés aux technologies émergentes (intelligence artificielle, infonuagique), conformité (DORA, RGPD) et formateur accrédité de l'ISACA

DORA (Digital Operational Resilience Act) renforce la résilience numérique des entités financières de l'Union européenne via cinq piliers (risque, incident, maitrise des tiers, tests techniques, partage d'informations).

Le défi majeur réside dans l'audit : définir précisément son périmètre couvrant toutes les infrastructures critiques et se conformer aux normes techniques et aux délais stricts imposés pour 2025.

En 2024, le coût de la cybercriminalité dans le monde atteint 14,57 trillions de dollars et devrait grimper à 17,65 trillions en 2025, selon des sources comme Statista, le FBI et le FMI.

Chaque année, ce coût augmente de 3 trillions de dollars supplémentaires.

Le secteur financier est particulièrement vulnérable aux cyberattaques en raison des gains potentiels élevés pour les cybercriminels. Ces attaques peuvent être provoquées par divers facteurs, qu'il s'agisse d'incidents involontaires ou d'attaques intentionnelles.

Les ransomwares (rançongiciels), le phishing (hameçonnage) et les attaques par déni de service distribué (DDOS) figurent parmi les trois principales menaces pesant sur le secteur financier dans la catégorie des risques opérationnels.

Pour renforcer la résilience face à ces menaces, la réglementation DORA a été mise en place, englobant 21 entités financières, des établissements de crédit aux prestataires de services tiers.

Cette nouvelle réglementation impose des défis de taille à l'équipe d'audit interne, qui doit monter en compétence et s'approprier les exigences réparties sur cinq piliers principaux.

Pilier 1 – Gestion des risques liés aux technologies de l'information et de la communication (TIC)

Dans le cadre du premier pilier de DORA, l'audit interne joue un rôle crucial en adoptant une approche fondée sur les risques pour évaluer et renforcer la stratégie de résilience opérationnelle numérique. Cela inclut la vérification de la conformité des politiques de gestion des risques TIC ainsi que l'efficacité des mécanismes de gouvernance, de confidentialité, d'intégrité et de disponibilité des données et des plans de continuité et de réponse aux incidents liés aux TIC.

Pilier 2 – Gestion, classification et notification des incidents TIC et des cybermenaces

L'audit interne doit également garantir la conformité avec la nouvelle méthodologie standard de classification des incidents introduite par DORA, en vérifiant que les critères spécifiques (tels que le nombre d'utilisateurs affectés, la durée et l'impact économique) sont correctement appliqués.

Pilier 3 – Tests de résilience opérationnelle numérique

Pour ce troisième pilier, l'auditeur interne est appelé à adopter une approche plus fréquente, exhaustive et sophistiquée des tests de résilience opérationnelle numérique. Cela nécessite une étroite collaboration avec la direction et les tiers pour évaluer la maturité des processus de l'organisation et assurer la conformité aux exigences réglementaires de DORA.

Pilier 4 – Gestion des risques liés aux prestataires de services TIC

DORA impose à l'audit interne d'effectuer une évaluation plus approfondie et systématique des contrats avec les prestataires de services TIC.

Cette évaluation comprend la vérification de clauses spécifiques, l'examen des plans de sortie et l'audit continu de la conformité des fournisseurs aux normes de sécurité et de résilience opérationnelle.

Pilier 5 – Partage d'informations en matière de cybersécurité

Enfin, l'audit interne doit évaluer l'efficacité et la conformité des processus de partage d'informations sur les menaces et les vulnérabilités. Cela implique de s'assurer que la collaboration sectorielle est bien équilibrée avec la protection des données sensibles de l'organisation.

La nouveauté et la particularité de DORA concernant l'audit interne résident dans plusieurs aspects :

- Renforcement du rôle et de l'indépendance : DORA exige explicitement « une séparation et une indépendance adéquates des fonctions de gestion du risque lié aux TIC, des fonctions de contrôle et des fonctions d'audit interne ». Cela renforce le rôle de l'audit interne comme une fonction véritablement indépendante.
- Attention accrue sur les risques TIC : l'audit interne doit désormais intégrer de manière plus approfondie l'évaluation des risques liés aux TIC dans son périmètre.
- Fréquence et exhaustivité accrues : le cadre de gestion du risque doit être « révisé et audité tous les ans », impliquant une fréquence plus élevée et une couverture plus complète des audits liés aux TIC.
- Implication de la direction : DORA souligne la responsabilité de l'organe de direction dans la supervision et la mise en œuvre du cadre de gestion des risques, ce qui implique une interaction plus étroite entre l'audit interne et la direction.

- Expertise technique renforcée : les auditeurs internes doivent développer une expertise plus poussée en matière de cybersécurité et de résilience opérationnelle numérique pour répondre aux exigences de DORA.
- Approche plus holistique : l'audit interne doit adopter une vision plus globale, intégrant non seulement les aspects techniques, mais aussi la gouvernance, la formation du personnel et la gestion des prestataires tiers.
- Ces changements impliquent une évolution significative du rôle de l'audit interne, le plaçant au cœur de la stratégie de résilience opérationnelle numérique des entités financières.

- Approche plus holistique : l'audit interne doit adopter une vision plus globale, intégrant non seulement les aspects techniques, mais aussi la gouvernance, la formation du personnel et la gestion des prestataires tiers.
- Ces changements impliquent une évolution significative du rôle de l'audit interne, le plaçant au cœur de la stratégie de résilience opérationnelle numérique des entités financières.

La réglementation DORA marque un tournant majeur pour la résilience informatique des entités financières en renforçant la gouvernance, la gestion des risques TIC et la collaboration entre l'audit interne et la direction. Dans un contexte d'augmentation rapide des cybermenaces, elle impose une approche plus rigoureuse, fréquente et holistique de l'audit, exigeant une expertise accrue en cybersécurité. DORA place ainsi l'audit interne au centre de la stratégie de résilience opérationnelle, garantissant une protection renforcée contre les risques numériques et une adaptation continue aux défis croissants de la cybersécurité.

Teddy Ramanakasina

Professionnel en sécurité informatique avec 30 ans d'expérience et expert en gestion des risques, en audit et en cybersécurité ayant occupé des postes de direction chez Nokia, Nortel, Alcatel, Orange, Sodexo et EY dans les secteurs des télécommunications et des banques.

https://www.ey.com/

Guide d'audit pour renforcer la résilience face à DORA

Pour mener à bien un audit interne conforme à la réglementation DORA, il est essentiel de suivre une méthodologie structurée qui comprend plusieurs étapes clés :

1. **Définir le périmètre d'audit :** la première étape consiste à déterminer si l'entité à auditer relève du périmètre de DORA. L'article 2 de la réglementation énumère 21 types d'institutions couvertes. Cette étape permet de confirmer la nécessité de l'audit.
2. **Identifier les fonctions critiques et importantes (CIF) :** il est crucial que l'entreprise ait défini ses CIF, c'est-à-dire des activités dont l'interruption pourrait gravement perturber les opérations de l'entité ou la stabilité financière dans l'Union européenne. Parmi ces fonctions figurent les services de paiement, la gestion de la liquidité, les services de cloud computing, (infonuagique) etc.
3. **Sélectionner les articles réglementaires à auditer :** l'audit doit porter sur les articles pertinents de DORA, tels que les suivants :
    - Articles 5-16 : gestion des risques TIC;
    - Articles 17-23 : gestion des incidents TIC et des cybermenaces;
    - Articles 24-27 : tests de résilience opérationnelle numérique;
    - Articles 28-44 : gestion des risques liés aux prestataires TIC;
    - Article 45 : partage d'informations en cybersécurité.
4. **Choisir les RTS, les ITS et les guidelines (lignes directrices) applicables :** l'audit doit se baser sur les 8 RTS (regulatory technical standards), 2 ITS (implementation technical standards) et 2 guidelines (lignes directrices) spécifiques à DORA.
5. **Faire un mapping des contrôles :** un rapprochement des contrôles de DORA avec des référentiels existants comme ISO 27002 et COBIT 2019 est nécessaire pour garantir une couverture exhaustive des risques.
6. **Conduire l'audit selon les étapes classiques :** l'audit se déroule en quatre phases, soit la préparation (programme de travail, lettre de mission), la phase terrain (collecte de preuves), la restitution (rapport d'audit avec constats et recommandations) et le suivi des recommandations.

Bâtir des entreprises antifragiles

Votre entreprise peut-elle transformer les crises en opportunités de croissance ?

Découvrez comment l'antifragilité, bien au-delà de la résilience, peut renforcer vos systèmes, relations et innovations.

Cet article vous guide, à travers une pyramide inspirée de Maslow, pour prospérer dans un monde en perpétuelle évolution.

Interview 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.

Dans un environnement en constante évolution, les entreprises ne peuvent plus se contenter de survivre aux crises. Elles doivent prospérer grâce à elles. C'est là qu'intervient le concept d'antifragilité : la capacité à se renforcer et à s'améliorer face aux perturbations. Contrairement à la résilience, qui vise à résister et à rebondir après une crise, l'antifragilité transforme les défis en opportunité de croissance.

Cet article adapte la pyramide des besoins de Maslow pour identifier et hiérarchiser les stratégies visant à renforcer la capacité de l'entreprise non seulement à faire face aux risques contemporains – cybernétiques, climatiques et sociaux –, mais aussi à en tirer parti pour se développer. Cette approche en cinq niveaux va des fondamentaux opérationnels et financiers à l'innovation et à la croissance, en passant par la sécurité, les relations et la reconnaissance.

L'objectif est de fournir aux dirigeants, aux gestionnaires de risques et aux professionnels de la planification stratégique des pistes de réflexion pour comprendre et intégrer l'antifragilité dans toutes les facettes de leur organisation. En naviguant à travers les différents niveaux de la pyramide, nous partagerons des stratégies concrètes pour construire des organisations capables de prospérer dans l'incertitude et de se renforcer face aux défis de demain.

1. Besoins opérationnels et financiers

La pérennité d'une entreprise repose sur ses besoins opérationnels et financiers, à la base de la pyramide de Maslow.

Dans un environnement volatil marqué par des risques cybernétiques, climatiques et sociaux, sécuriser ces besoins est prioritaire.

Sécurité des transactions et protection des actifs

À l'ère numérique, la protection des actifs numériques est cruciale. Les cyberattaques ne sont pas seulement des menaces à neutraliser, mais des opportunités pour améliorer les systèmes de sécurité. Par exemple, lorsqu'une entreprise subit une attaque, elle peut en tirer des leçons pour renforcer ses défenses et former ses employés aux dernières menaces. Investir dans des technologies avancées, former continuellement les employés et développer des politiques de gestion des données robustes permettent à l'entreprise de se renforcer face aux cybermenaces.

Assurances et fonds de secours

Les événements climatiques extrêmes posent des risques pour les opérations et les infrastructures. Assurances adaptées et fonds de secours sont essentiels pour atténuer les impacts financiers. Une entreprise qui a bien géré une inondation récente en utilisant ces outils peut servir d'exemple. Une stratégie proactive de gestion des risques climatiques, comprenant l'évaluation des couvertures d'assurance et la création de réserves financières, permet non seulement de se protéger, mais aussi d'anticiper les futurs défis climatiques et de mieux y répondre.

Flexibilité opérationnelle

La flexibilité opérationnelle est un indicateur clé d'antifragilité. Les entreprises doivent adopter des modèles de travail flexibles, diversifier leurs chaînes d'approvisionnement et ajuster leurs stratégies commerciales pour transformer les crises en opportunité de développement. Par exemple, une entreprise de fabrication qui a diversifié ses fournisseurs pendant la pandémie non seulement a survécu, mais a aussi trouvé de nouveaux partenaires stratégiques. Cette agilité opérationnelle permet de minimiser les perturbations et de saisir de nouvelles opportunités sur des marchés en mutation.

2. Besoins de sécurité

La sécurité représente le deuxième niveau de la pyramide, assurant la stabilité face aux menaces.

Une entreprise antifragile utilise les menaces comme des leviers pour se renforcer.

Cybersécurité et protection des données

Assurer la sécurité des données est primordial. Une infrastructure de technologie de l'information (TI) robuste doit intégrer des mesures de cybersécurité avancées qui non seulement protègent contre les intrusions, mais aussi apprennent et s'améliorent de chaque tentative de violation. Politiques de sécurité des informations et formations régulières sont essentielles pour une défense proactive.

Plans de continuité d'activité

Les catastrophes naturelles et les cyberattaques peuvent avoir des impacts dévastateurs. Mettre en place des plans de continuité d'activité (PCA) robustes assure une reprise rapide. Une entreprise antifragile utilise ces plans non seulement pour reprendre ses activités, mais aussi pour identifier des points faibles et les convertir en forces. Par exemple, une entreprise de logistique qui teste et améliore régulièrement son PCA peut maintenir ses activités pendant une grande panne de réseau.

Gestion des risques sociaux

Les changements législatifs et les mouvements sociaux affectent les activités. Une stratégie de gestion des risques sociaux implique une veille réglementaire active pour anticiper ces changements. Engagement avec les communautés, initiatives de responsabilité sociale d'entreprise (RSE) et politiques internes pour promouvoir l'équité sont essentiels. Les entreprises antifragiles voient ces interactions comme des moyens de renforcer leur position et de s'adapter aux nouvelles normes sociétales. Un bon exemple est une entreprise de technologie qui, en répondant activement aux mouvements pour l'égalité sociale, a amélioré sa culture d'entreprise et son image publique.

3. Besoins relationnels

Les besoins relationnels soulignent l'importance des interactions avec les parties prenantes, qui incluent les employés, les clients, les fournisseurs et la communauté.

Cultiver des relations solides basées sur la confiance et l'engagement environnemental contribue à la croissance durable et à l'antifragilité.

Confiance et transparence avec les parties prenantes

Un dialogue ouvert et transparent est crucial. Communiquer clairement sur les mesures de sécurité et d'engagement renforce les relations basées sur la confiance.

Les entreprises antifragiles tirent parti de ces interactions pour améliorer continuellement leurs processus et renforcer leurs réseaux de soutien. Par exemple, une entreprise qui communique ouvertement avec ses clients sur ses politiques de confidentialité peut renforcer la fidélité et la confiance de ceux-ci.

Engagement pour la responsabilité environnementale

Adopter des pratiques durables montre un engagement envers la préservation de l'environnement. Réduction de l'empreinte carbone, recyclage et utilisation d'énergies renouvelables renforcent l'image de marque et encouragent une culture de la durabilité. Pour une entreprise antifragile, ces pratiques sont des opportunités d'innovation et de leadership environnemental.

Par exemple, une entreprise de mode qui intègre des matériaux recyclés dans ses produits réduit son impact environnemental et attire une clientèle soucieuse de l'écologie.

Renforcement des liens communautaires

L'engagement communautaire implique de construire des relations significatives. Mise en œuvre de programmes de bénévolat, soutien à des initiatives locales et participation à des projets de développement communautaire montrent que l'entreprise valorise son environnement social.

Les entreprises antifragiles utilisent ces engagements pour renforcer leur résilience et leur capacité à s'adapter aux changements sociaux. Une entreprise de grande

4. Besoins de reconnaissance

Les besoins de reconnaissance établissent l'entreprise comme un leader.

La reconnaissance va au-delà de la notoriété de la marque pour inclure la réputation de l'entreprise en matière de sécurité et d'engagement social et environnemental.

Développement d'une marque sécurisée

Construire une réputation solide autour de la sécurité nécessite l'adoption de mesures de cybersécurité et une communication transparente. Les entreprises modèles en sécurité inspirent la confiance et renforcent leur valeur de marque. L'antifragilité permet d'utiliser chaque défi de sécurité pour démontrer et renforcer cet engagement. Par exemple, une entreprise qui publie régulièrement des rapports de transparence sur sa cybersécurité peut gagner la confiance des investisseurs.

Obtention de certifications environnementales

Les certifications comme ISO 14001 ou B Corp démontrent l'engagement envers la durabilité. Elles attirent des consommateurs soucieux de l'écologie et établissent des normes sectorielles en matière de pratiques durables. Les entreprises antifragiles cherchent à obtenir et à dépasser ces certifications pour rester à la pointe de l'innovation durable. Par exemple, une entreprise alimentaire qui obtient une certification peut se distinguer sur le marché et attirer des talents qui partagent ses valeurs.

Leadership dans la réponse aux enjeux sociaux

Prendre position sur des questions sociales et intégrer la responsabilité sociale dans le modèle d'affaires distinguent les entreprises comme des leaders. Promouvoir l'égalité des chances et répondre aux défis sociaux renforcent l'image de marque et l'engagement des parties prenantes. Les entreprises antifragiles transforment ces enjeux en opportunités de croissance et d'innovation sociale. Une entreprise technologique qui s'engage pour l'inclusion et la diversité peut créer un environnement de travail plus dynamique et innovant.

5. Besoins d’innovation et de croissance

Au sommet de la pyramide se trouvent les besoins d’innovation et de croissance.

L’innovation en cybersécurité, le développement de produits durables et l’adaptation aux changements sociaux assurent la croissance continue et la compétitivité à long terme.

Avancées en cybersécurité

L’innovation continue en matière de cybersécurité est nécessaire pour devancer les cybermenaces. Investir dans la recherche et le développement de nouvelles technologies de sécurité renforce la protection des actifs et la position de l’entreprise comme leader innovant. Pour les entreprises antifragiles, chaque nouvelle menace est une occasion d’améliorer et d’innover. Par exemple, une entreprise qui développe une nouvelle technologie de détection de menaces peut se positionner en tant que leader sur le marché de la cybersécurité.

Développement de produits et services durables

L’innovation en durabilité est un impératif stratégique. Utilisation de matériaux recyclés, conception de produits économes en énergie et recherche de solutions contribuant à une économie circulaire répondent aux préoccupations climatiques et ouvrent de nouvelles opportunités de marché. Les entreprises antifragiles voient ces initiatives comme des leviers de croissance et de différenciation sur le marché. Par exemple, une entreprise d’électronique qui lance une gamme de produits écoresponsables peut attirer une clientèle soucieuse de l’environnement.

Réponse aux changements sociaux

Innover pour répondre aux changements sociaux signifie développer des produits et services reflétant la diversité et l’inclusion. Pratiques commerciales éthiques et engagement dans des initiatives sociales renforcent la réputation et répondent aux attentes de la société. Les entreprises antifragiles utilisent ces changements pour se renforcer et développer de nouvelles opportunités occasions d’affaires. Une entreprise de services financiers qui adapte ses offres pour mieux répondre aux besoins des populations marginalisées peut non seulement élargir sa base de clients, mais aussi renforcer son image de marque.

La pyramide des besoins essentiels d'une entreprise orientée sur l'antifragilité met en lumière la hiérarchie des priorités pour bâtir une organisation capable de prospérer face aux défis contemporains. Intégrer l'antifragilité comme composante essentielle de la stratégie globale est une nécessité.

Une approche holistique, reconnaissant l'interconnexion entre la sécurité financière et opérationnelle, la stabilité des relations, la réputation et l'innovation, est essentielle pour naviguer dans un environnement complexe et incertain. Les entreprises qui adoptent cette vision, investissant dans chaque niveau de la pyramide, se mettent dans une position où elles peuvent non seulement gérer efficacement les crises, mais aussi en émerger plus fortes et robustes.

L'antifragilité doit être vue non pas comme une série de tactiques réactives,
mais comme une stratégie proactive et intégrée, plaçant les concepts au cœur de leur mission
pour construire un avenir durable et prospère.

Alexandre Fournier

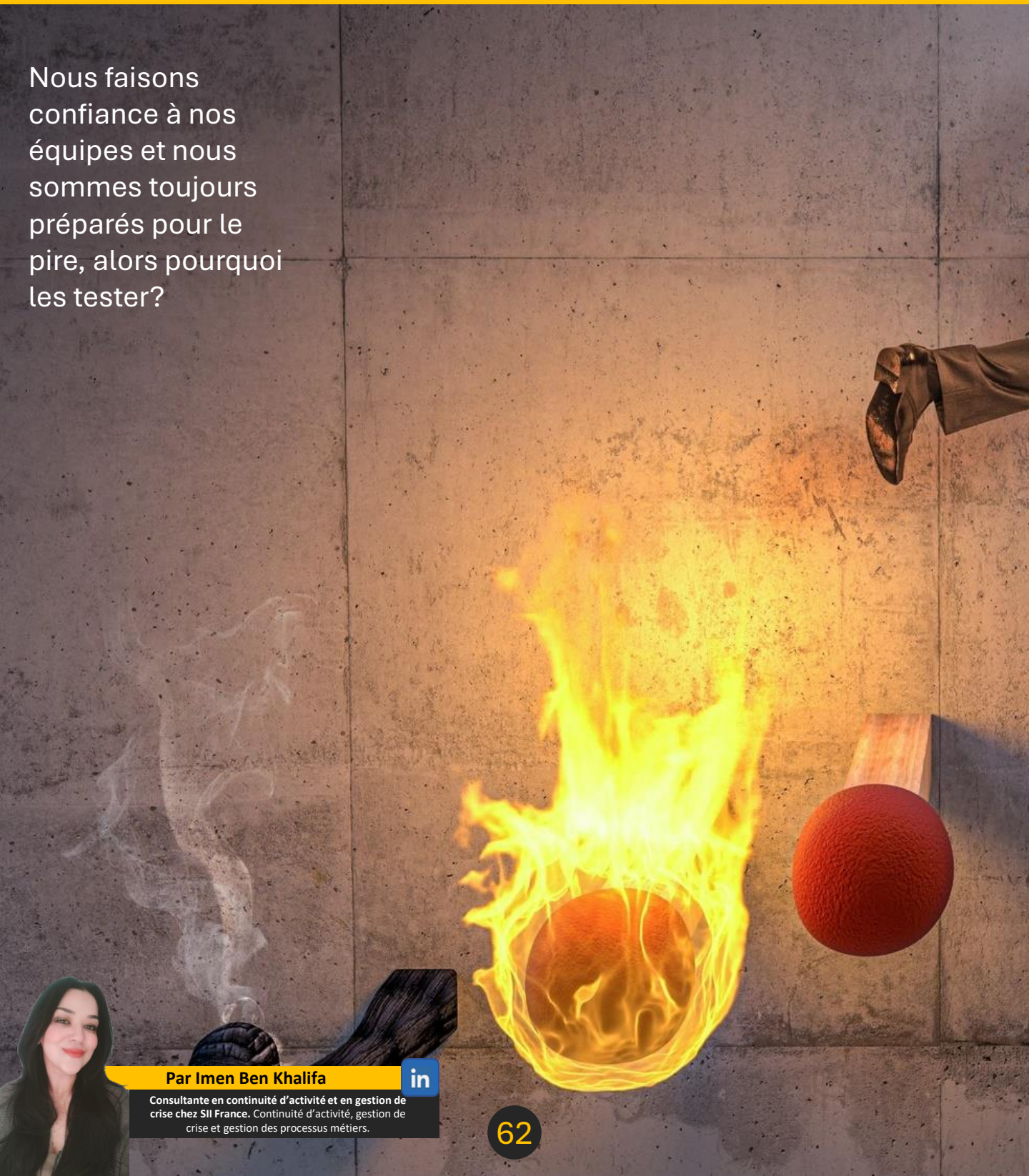
CRISE & RÉSILIENCE
L'ART DE SURVIVRE AUX CRISES

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

www.crise-resilience.com

Ces plans de continuité d'activité « théoriquement » résilients…

Nous faisons confiance à nos équipes et nous sommes toujours préparés pour le pire, alors pourquoi les tester?



Par Imen Ben Khalifa

Consultante en continuité d'activité et en gestion de crise chez SII France. Continuité d'activité, gestion de crise et gestion des processus métiers.

Face aux risques de plus en plus importants dans la société d'aujourd'hui, notamment les risques naturels, technologiques ou aussi sociopolitiques, les organismes publics et privés de tous les secteurs trouvent nécessaire d'accentuer leur résilience au-delà des mesures à court terme, préservant ainsi leurs capitaux humains et physiques.

Avec toutes les bonnes intentions et la meilleure des volontés…

Avec cette prise de conscience des conséquences et des impacts graves sur leurs services et leurs activités en cas de survenue d'une situation critique, les administrations, les autorités publiques et les dirigeants des entreprises commencent à agir. Ils rajoutent à l'organigramme une nouvelle organisation et y font embarquer ceux qui rédigent et mettent en place les plans de continuité et de gestion de crise miracles.

Ces plans « théoriques » sont perçus comme des bouées de sauvetage qui seront retirées des tiroirs pour sauver l'entreprise dans les plus brefs délais pendant les temps durs.

Alors un jour, le responsable de la continuité d'activité et le gestionnaire de crise demandent à leurs responsables de créer l'incertitude, de vérifier l'efficacité des plans, de s'assurer que les fonctionnements décrits et les schémas d'alerte et de mobilisation couvrent les périmètres définis et répondent au mieux aux attentes de la direction, ainsi que de repérer et de corriger les points faibles dans ce dispositif de protection. Se préparer au pire et créer la pression d'urgence comme dans une situation réelle et incertaine, disaient-ils.

Mais, mauvaise surprise, la préservation de la valeur a un coût. Et ce coût s'avère cher pour les organismes.

Quand les budgets manquent…

Anticiper la crise est le meilleur moyen de réduire son impact le jour où l'événement critique survient, et ce travail d'anticipation se fait naturellement avec l'organisation périodique et régulière d'exercices de simulation de crise, qui deviennent de plus en plus diversifiés et complexes.

Mais la pression durable et globale qu'exerce le nouveau paradigme des « contraintes budgétaires » sur la ligne managériale est plus forte que tout. La ligne directrice est désormais « être efficace en réduisant les dépenses ».

Cela appelle ainsi les dirigeants à gérer autrement, à faire confiance aux avis et à l'expérience des équipes opérationnelles, et à croire en leurs capacités théoriques de réponse et d'adaptation en situation de crise.

Pas de choix pour la direction, et pas de chance pour les collaborateurs qui souhaitent confirmer ces connaissances théoriques. Pas de chance pour ceux qui veulent développer les réflexes nécessaires qui serviront à appréhender les crises. Pas de chance pour mettre à l'épreuve tous les niveaux de l'organisation.

Et d'ici naît une culture de résilience incomplète, une culture de continuité d'activité et de gestion de crise qui reste, malgré tout, théorique.

Les exercices trop lourds traduisent des objectifs vagues ou trop nombreux

Comment rendre rentable un exercice ou une simulation de crise?

Les exercices trop lourds traduisent des objectifs vagues ou trop nombreux. Alors, pour que la méthode d'élaboration d'un exercice ou d'une simulation de crise soit efficace et rentable pour la direction, la première exigence à respecter consiste à bien clarifier l'objectif et les besoins spécifiques de cet exercice, qui doivent être adaptés à la réalité opérationnelle de l'entreprise.

L'exercice peut être minimaliste et réalisé uniquement « sur table », en transverse, en faisant participer les bonnes équipes opérationnelles. Cela permet de se rassurer dans une première étape.

Chaque exercice doit reposer sur un scénario évolutif et veiller à ne pas reproduire des schémas d'entraînement existants.

Ces exercices doivent être considérés comme étant une opportunité qui tend à développer les automatismes et les réflexes en situation d'urgence. Cela permet également de renforcer l'esprit d'équipe et d'augmenter la confiance en soi.

Un programme de sensibilisation et de formation, à tous les niveaux de l'organisation, au sujet des bonnes pratiques à adopter face aux risques majeurs doit être déployé.

Et, à la fin, les plans mis en place doivent être revus systématiquement pour s'adapter en permanence au contexte de l'entreprise et aux changements internes ou externes.

Du risque à la réalité…

Le passage de la théorie et de la construction de la réalité à une vraie situation de crise est un événement potentiellement déstabilisateur pour les organismes publics et les entreprises.

La survie ne tient qu'à deux fils, soit la réactivité des dirigeants et les compétences opérationnelles des collaborateurs.

La question reste : est-ce encore possible de croire que la continuité des activités est vraiment acquise?

Imen Ben Khalifa

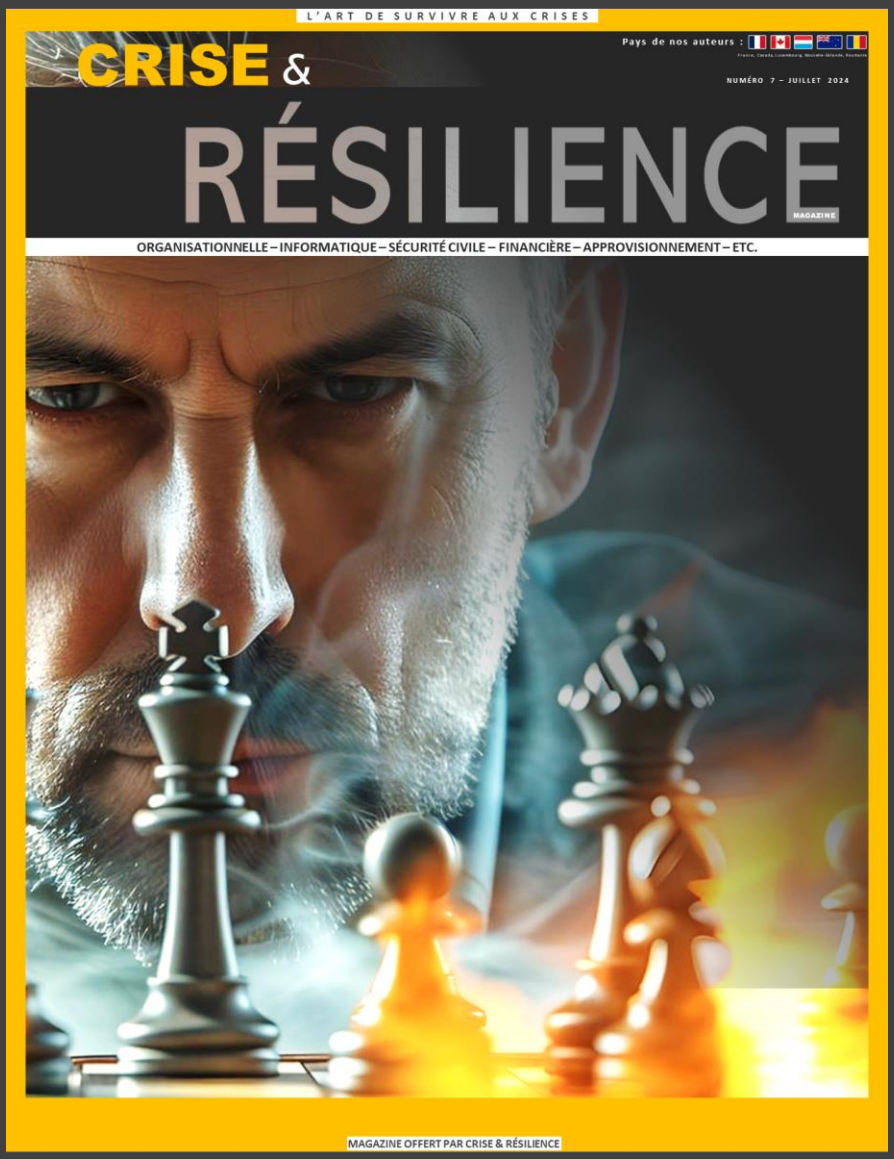
Titulaire d'un diplôme d'ingénieur et d'un MBA International Paris, je suis dotée aujourd'hui d'une forte expérience professionnelle en continuité d'activité, en gestion de risques, en gestion de crises et en gestion de projets, et j'ai géré dernièrement des projets de grande envergure, notamment avec la réalisation des exercices de simulation de crise dans le cadre des projets « Paris à 50 °C » et « Crue de Seine ».

https://www.linkedin.com/in/imenbenkhalifab/

En complément de cet article, vous pouvez Lire le dossier du mois de juillet

www.criseetresilience-magazine.com/

RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

www.CriseEtResilience-Magazine.com