

**CRISE** &

# RÉSILIENCE

MAGAZINE

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

**L'espionnage industriel dans une PME**

Ce n'est pas du cinéma!

**Données possiblement « perdues » ?**

Voici la solution de la dernière chance!

**Improvisation en gestion de crise**

Bonne ou mauvaise idée?

**Intégrer l'intelligence artificielle**

pour améliorer sa résilience  
et sa gestion de crise!

**Sécurité de l'information**

Le mirage de la cybersécurité  
et de la confidentialité

**Le coordinateur de crise**

Le casting stratégique!

**DOSSIERS DU MOIS**

**Risques climatiques, une  
approche globale devenue vitale**

CRISE &

# RÉSILIENCE

C'EST...  
AUSSI

Une chaîne  YouTube avec...

Des conférences et formations gratuites



Des interviews d'experts :

 <p><b>D'EXPERTS</b> Déjouer les risques. 5 idées vraies pistes pour les c... 1:21:23</p> <p>Raphaël De Vittoris</p>	 <p><b>D'EXPERTS</b> Comment apporter les techniques du survivalisme à l'en... 34:49</p> <p>Mathieu Montaroux</p>	 <p><b>D'EXPERTS</b> Le rôle du Responsable de Continuité d'Activité 42:15</p> <p>Cécile Weber</p>	 <p><b>PAROLE D'EXPERTS</b> Cyberattaque 14:49</p> <p>Quelles sont les erreurs à ne pas...</p>	 <p><b>PAROLE D'EXPERTS</b> NEGOTIATION négocier avec les cyber... 46:17</p> <p>Julien Lazard</p>
Comment déjouer les risques : - 5 idées reçues - Interview...	Comment apporter les techniques du survivalisme ...	Gestion de Crise & Continuité des Activités: Expertise de...	Cyberattaque : Les erreurs à ne pas faire - Parole d'exper...	Les conseils d'un expert pour faire face aux demandes de...

Des réponses à vos questions :

 <p><b>LA QUESTION DU LUNDI</b> C'est quoi la Cyber Résilience? Versus la Cyber sécurité... 2:39</p>	 <p><b>La question du Lundi</b> Pourquoi notre logo est une fourmi? 3:07</p>	 <p><b>LA QUESTION DU LUNDI</b> Assurance et/ou plan de continuité? 2:10</p>	 <p><b>LA QUESTION DU LUNDI</b> Est-ce trop tard pour un plan de continuité? 3:27</p>	 <p><b>LA QUESTION DU LUNDI</b> Êtes-vous un poisson? HAMEÇONNAGE PARTIE 1 Les pièges 2:42</p>
C'est quoi la Cyber Résilience et quelle différence avec...	Pourquoi notre Logo est une fourmi   Rapport avec la...	Plan de continuité d'activité et/ou assurance	Plan de continuité des affaires est-ce trop tard pou...	Hameçonnage et continuité des affaires - Quel sont les...

Une page  avec...

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



*Chers lecteurs,*

C'est avec un immense enthousiasme que nous vous présentons ce nouveau numéro de "Crise & Résilience", riche en analyses approfondies et en témoignages d'experts pour vous aider à renforcer la résilience de votre organisation face à l'imprévisible.

Dans un monde où les défis se multiplient, des cybermenaces grandissantes aux catastrophes naturelles exacerbées par le dérèglement climatique, ce magazine se veut un guide précieux pour anticiper et surmonter les crises majeures.

Le dossier du mois, réalisé par Walter Munsch, explore en profondeur les risques climatiques systémiques et l'urgence d'adopter une approche globale pour y faire face.

Alexandre Fournier nous éclaire sur le potentiel de l'intelligence artificielle pour révolutionner la gestion de crise, de la détection précoce des risques à la planification agile de réponses.

Karine Maréchal-Richard explore l'art subtil de l'improvisation en situation de crise, compétence désormais cruciale pour les gestionnaires pour réagir avec créativité et agilité mentale face à l'inattendu.

Anne-Gervaise Vendange met en lumière le rôle primordial du coordinateur de cellule de crise, véritable chef d'orchestre dont le bon choix peut faire toute la différence dans l'efficacité de la gestion de crise.

Dans un registre différent, mais tout aussi essentiel, Philippe Chevalier nous alerte sur les risques d'espionnage industriel qui guettent même les PME, partageant ses conseils avisés pour détecter et contrer ces menaces insidieuses.

Francis Coats, Frédéric Loisel, Dimitri Souleliac et Christophe Vanypre abordent ensuite les défis de la cybersécurité, de la préparation aux cyberattaques à la récupération cruciale des données après une attaque par rançongiciel. Des perspectives riches et complémentaires pour renforcer notre cyber-résilience.

Enfin, Jean François Jund nous livre un éclairage instructif sur l'importance vitale des tests de plans de continuité d'activité, illustré par le cas de la Roumanie face aux risques sismiques et cyber.

En ces temps d'incertitudes, ce numéro foisonnant vous apporte les clés pour transformer les défis en opportunités de croissance durable. Nous espérons que ces analyses d'experts vous inspireront et vous guideront vers plus de résilience organisationnelle.

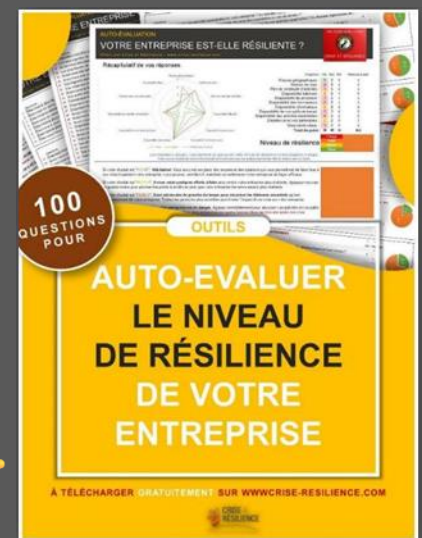
*Bonne lecture à tous !*

*L'équipe éditoriale*

Intégrer l'intelligence artificielle pour améliorer sa résilience et sa gestion de crise	Alexandre Fournier	04
Improvisation en gestion de crise - Bonne ou mauvaise idée ?	Karine-Maréchal Richard	08
<b>Dossier du mois</b> – Risques climatiques, une approche globale devenue vitale	Walter Munsch	14
Le coordinateur de crise, le casting stratégique!	Anne-Gervaise Vendange	28
L'espionnage industriel dans une PME? Ce n'est pas du cinéma!	Philippe Chevalier	32
Sécurité de l'information : le mirage de la cybersécurité et de la confidentialité	Francis Coats	36
Vendredi 17 h 48 mon ordinateur ne fonctionne plus et toi ...	Frédéric Loisel	40
Cyber-résilience - Point de vue d'ici et d'ailleurs	Dimitri Souleliac	46
Données possiblement « perdues » ? Voici la solution de la dernière chance!	Christophe Vanypre	50
<b>La chronique</b> – Relaxation	Timothy Mirthil-de Segonzac	54
Roumanie, à quoi bon un PCA sans test?	Jean-François Jund	56

Envie de  
connaître  
votre niveau  
de résilience ?

Réaliser votre  
auto-évaluation  
En cliquant ici



Version flip en ligne sur

[www.criseetresilience-magazine.com](http://www.criseetresilience-magazine.com)

# Intégrer l'intelligence artificielle pour améliorer sa résilience et sa gestion de crise

Découvrez comment l'intelligence artificielle (IA) transforme la gestion de crise et la résilience des entreprises.

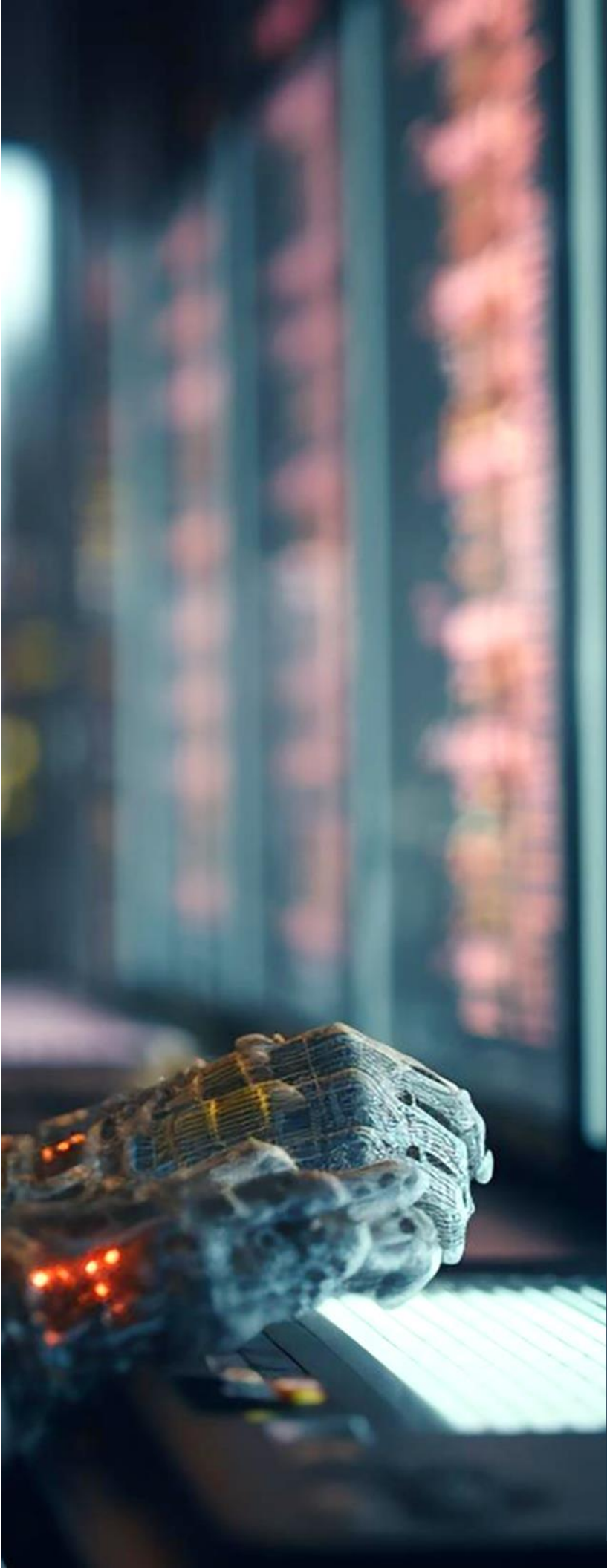
De la détection anticipée des risques à la planification agile, l'IA promet une révolution dans la préparation et la réaction aux événements imprévus.



par **Alexandre Fournier**



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



L'exploration des potentialités de l'intelligence artificielle (IA) dans le domaine de la continuité des affaires et de la résilience opérationnelle ouvre des perspectives fascinantes sur la manière dont les entreprises pourraient anticiper les risques et gérer les crises à l'avenir.

### Révolution prédictive et gestion de crise

Avec ses avancées technologiques, l'IA pourrait révolutionner la préparation, la réaction et la récupération face à des événements imprévus en exploitant des technologies telles que le machine *learning*, le *deep learning* et le traitement automatique du langage naturel.

L'IA démontre déjà un potentiel dans l'identification et l'analyse de risques conventionnelles. Elle excelle particulièrement dans la surveillance continue des flux de données, permettant la détection précoce d'anomalies indicatives de risques imminents. Cette capacité d'anticipation, fondée sur l'analyse rapide et précise d'importants volumes de données, offre l'occasion de mettre en place des actions préventives efficaces.

Grâce à des technologies avancées comme le machine *learning* et l'analyse prédictive, l'IA analyse les tendances passées et présentes pour prédire avec une grande justesse les événements futurs, tels que les variations du marché ou les catastrophes naturelles.

Cette prévoyance pourrait équiper les entreprises des outils nécessaires pour se préparer à l'avance, renforçant ainsi leur capacité à prévenir les crises avant leur apparition et à se mouvoir avec agilité dans un paysage commercial volatile.

Au cœur de cette révolution prédictive, l'IA se manifeste à travers plusieurs applications clés :

- **Surveillance dynamique** : par un examen minutieux et continu des données, l'IA identifie les signaux avant-coureurs de risques, y compris les vulnérabilités de sécurité, les mouvements de marché négatifs ou les fragilités au sein de la chaîne d'approvisionnement.
- **Anticipation des mouvements de marché** : utilisant des modèles prédictifs, l'IA prévoit les tendances de marché, permettant aux entreprises d'ajuster leurs stratégies en amont face à des changements économiques.
- **Alerte précoce des phénomènes naturels** : grâce à des modèles climatiques et à des données environnementales, l'IA peut prédire les catastrophes naturelles, accordant aux entreprises le temps nécessaire pour consolider leurs plans de préparation.

La gestion de crise représente, elle aussi, un domaine où l'IA pourrait véritablement briller, offrant des capacités jusqu'alors inexplorées. Voici quelques-unes des manières dont l'IA pourrait transformer la gestion de crise :

- **Détection et réponse automatisée** : en utilisant l'IA pour surveiller des systèmes et des flux de données en temps réel, les entreprises pourraient détecter automatiquement des anomalies signalant une crise imminente. L'IA pourrait alors déclencher des protocoles de réponse préprogrammés, accélérant considérablement le temps de réaction.
- **Simulation et planification de crise** : les systèmes d'IA pourraient simuler une gamme étendue de scénarios de crise, permettant aux entreprises de tester et d'affiner leurs plans de réponse.

# “L'IA démontre déjà un potentiel dans l'identification et l'analyse de risques conventionnelles.”

*Alexandre Fournier*

Ces simulations, basées sur des données historiques et des modèles prédictifs, pourraient révéler des faiblesses dans les stratégies actuelles et encourager le développement de plans plus robustes.

- **Analyse en temps réel et décision** : en cas de crise, l'analyse en temps réel effectué par l'IA pourrait fournir des informations critiques pour guider les décisions stratégiques. Cela inclut l'évaluation de l'impact, la priorisation des réponses et l'adaptation des stratégies en fonction de l'évolution de la situation.
- **Communication automatisée** : l'IA pourrait automatiser les communications avec les clients, les partenaires et le personnel durant une crise, assurant une diffusion rapide et cohérente des informations. Cela permettrait de libérer des ressources humaines pour se concentrer sur des aspects critiques de la gestion de crise.
- **Révision et adaptation postcrise** : après une crise, l'IA pourrait analyser les données pour identifier les leçons apprises, permettant aux entreprises d'ajuster leurs plans de continuité des affaires et de prévention des crises. Cette révision continue et l'apprentissage automatique de l'IA contribueraient à une amélioration constante des processus.

## **Anti-fragilité et progrès grâce à l'intelligence artificielle**

Le concept d'anti-fragilité, introduit par Nassim Nicholas Taleb, décrit des systèmes qui non seulement résistent au stress, aux chocs, à la volatilité, et aux perturbations, mais qui, en outre, s'améliorent et deviennent plus robustes en réponse à ceux-ci.

Contrairement à la simple résilience, qui vise à retourner à un état initial après une perturbation, l'anti-fragilité implique une capacité d'adaptation et d'évolution qui transforme les défis en opportunités de croissance et d'amélioration.

L'intelligence artificielle, avec ses capacités d'apprentissage et d'adaptation, peut jouer un rôle crucial dans le développement de systèmes anti-fragiles dans divers domaines, notamment les affaires, la finance, la santé, et la gestion des risques environnementaux.

- **Apprentissage et adaptation continus** : L'IA, grâce à l'apprentissage automatique et à d'autres formes d'apprentissage profond, peut continuellement apprendre de nouvelles données, s'adapter à des environnements changeants, et optimiser ses stratégies face à des défis inattendus. Cette capacité d'apprentissage et d'adaptation est au cœur de l'anti-fragilité, permettant aux systèmes de devenir plus intelligents et plus efficaces au fil du temps.

- **Détection et réponse rapides aux perturbations** : En identifiant des problèmes de manière proactive, l'IA peut aider à initier des réponses rapides et ciblées qui non seulement atténuent les effets immédiats de la perturbation, mais également renforcent le système contre de futures menaces.
- **Optimisation de la résilience à travers la diversification** : En analysant d'immenses volumes de données et en identifiant des tendances complexes, l'IA peut aider à concevoir des stratégies de diversification plus efficaces pour les investissements, les chaînes d'approvisionnement, et les écosystèmes numériques. Cette diversification, guidée par l'intelligence artificielle, peut réduire la vulnérabilité aux chocs spécifiques et contribuer à une anti-fragilité systémique.
- **Innovation et créativité** : Par son analyse avancée et sa capacité à modéliser des scénarios hypothétiques, l'IA peut ouvrir de nouvelles voies pour le développement de produits, services, et procédés qui non seulement répondent aux défis actuels, mais anticipent également les besoins futurs.
- **Renforcement de la capacité décisionnelle** : Cette capacité à anticiper et à modéliser divers scénarios permet une planification stratégique plus agile et adaptable, renforçant ainsi la capacité d'une organisation à prendre de meilleures décisions dans des environnements plus volatils.

Il est clair que l'intégration de l'intelligence artificielle (IA) dans les stratégies de continuité et de résilience des entreprises révolutionnera la gestion des risques et des crises.

Grâce à son aptitude à traiter de vastes ensembles de données pour prévoir les crises et automatiser les réponses, l'IA transforme la capacité des entreprises à anticiper et à réagir aux défis.

Elle ouvre une ère où la préparation aux crises atteint des niveaux sans précédent, tout en permettant aux organisations d'évoluer vers l'anti-fragilité, s'adaptant et se renforçant face aux perturbations.

Cette nouvelle ère de l'IA offre aux entreprises l'opportunité de non seulement sécuriser leur avenir dans un monde volatile, mais aussi de poursuivre une croissance et une innovation constantes.

**Alexandre Fournier**

Crise & Résilience, une entreprise québécoise leader en continuité des affaires et en gestion de crise, offre des services personnalisés, y compris des formations et du mentorat, pour renforcer la résilience opérationnelle des entreprises face à l'imprévisible.

[www.crise-resilience.com](http://www.crise-resilience.com)

**CRISE & RÉSILIENCE**  
L'ART DE SURVIVRE AUX CRISES

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

Autre article sur l'IA  
à lire  [Cliquez ici](#)

<https://www.criseetresilience-magazine.com/post/la-gestion-de-crise-%C3%A0-l-%C3%A8re-de-l-ia-avantages-limites-et-risques>

## 10 clés pour intégrer l'IA dans votre plan de continuité d'activité

Intégrer l'IA dans votre PCA peut transformer radicalement la manière dont votre entreprise anticipe et gère les crises. Voici 10 clés essentielles pour réussir cette intégration :

- **Surveillance prédictive des risques par l'IA** : mettez en œuvre des outils d'IA pour une surveillance continue et une évaluation dynamique des risques, captant des signaux précoces de vulnérabilités pour une gestion proactive.
- **Modèles prédictifs et anticipation** : investissez dans des modèles prédictifs sophistiqués pour prédire les changements de marché et les perturbations naturelles, assurant une préparation en avance sur les crises.
- **Plans de réponse évolués par l'IA** : utilisez l'analyse avancée pour développer des plans de réponse aux crises basés sur des simulations de scénarios variés, améliorant la résilience organisationnelle.
- **Détection des anomalies en temps réel** : intégrez l'IA pour une identification immédiate des anomalies, permettant une réaction rapide aux signaux avant-coureurs d'événements disruptifs.
- **Automatisation et réponse rapide** : mettez en place des protocoles de réponse automatisés pour une action immédiate suite à un incident, réduisant le délai d'intervention et optimisant l'exécution du PCA.
- **Gestion optimisée des ressources par l'IA** : utilisez des algorithmes d'IA pour une répartition stratégique des ressources pendant les crises, maximisant l'efficacité des interventions.
- **Communication intelligente en crise** : implémentez des solutions d'IA pour une communication automatisée et ciblée en temps de crise, assurant la cohérence et la rapidité de l'information transmise.
- **Préparation et simulations par l'IA** : conduisez des formations et simulations de crise basées sur l'IA pour entraîner le personnel, en exploitant les informations tirées des données pour un meilleur taux de réaction.
- **Retours d'expérience et amélioration continue** : post-crise, utilisez l'IA pour analyser les performances et intégrer les leçons apprises dans les procédures du PCA, affinant constamment les stratégies de réponse.
- **Intégrité et responsabilité de l'IA dans le PCA** : veillez à ce que l'implémentation de l'IA dans votre PCA respecte les plus hauts standards éthiques, en mettant l'accent sur la sécurité des données, la transparence des décisions prises par l'IA, et la responsabilité organisationnelle.

**ATTENTION, l'IA ne doit pas remplacer l'humain dans les décisions finales!**

# Improvisation en gestion de crise

## Bonne ou mauvaise idée ?

Alors que la complexité et l'imprévisibilité deviennent la norme, l'habileté à improviser de manière agile en période de crise émerge comme une aptitude essentielle pour les leaders et gestionnaires d'entreprise.



Par **Karine Maréchal-Richard** 

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





L'improvisation en gestion de crise se révèle être un art subtil, mêlant réactivité, créativité et prise de décision éclairée dans des contextes d'urgence et d'incertitude.

Face à des événements inattendus, à des catastrophes naturelles, à des crises sanitaires ou à des situations de conflit, la capacité à s'adapter rapidement et efficacement devient un atout majeur pour assurer la résilience et la survie des organisations.

### **Fondements théoriques de l'improvisation en gestion de crise**

L'improvisation en gestion de crise repose sur des fondements théoriques solides qui éclairent la manière dont les individus et les organisations réagissent et s'adaptent face à l'incertitude et à l'urgence.

Plusieurs chercheurs ont contribué à la compréhension de ce concept, mettant en lumière des aspects clés qui façonnent la pratique de l'improvisation en contexte managérial.

L'improvisation en gestion de crise peut être définie comme la capacité à réagir de manière créative et efficace face à des situations imprévues ou critiques, en utilisant les ressources disponibles de façon innovante.

Cette approche dynamique implique une adaptation rapide aux circonstances changeantes et une prise de décision agile pour faire face aux défis rencontrés.

### **Approches théoriques sur l'improvisation en gestion**

Selon Miguel Pina e Cunha, l'improvisation se caractérise par une utilisation novatrice des ressources, notamment en situation de crise. Il souligne l'importance d'une pensée flexible et d'une action rapide pour improviser efficacement dans des contextes complexes.

Quant à Karl E. Weick, il considère l'improvisation comme une compétence essentielle pour la planification de projets. Il met en avant la nécessité d'une coordination continue entre les phases de conception, de planification et d'exécution pour gérer efficacement les imprévus.

Au fil du temps, l'improvisation en gestion a évolué pour être perçue comme une compétence précieuse permettant aux organisations de s'adapter aux changements rapides et aux crises inattendues.

Les avancées technologiques, les pressions concurrentielles et les risques accrus ont renforcé la nécessité pour les gestionnaires d'être capables d'improviser avec agilité et créativité.

### **Compétences et stratégies d'improvisation en gestion de crise**

L'improvisation en gestion de crise requiert un ensemble de compétences spécifiques et l'utilisation de stratégies adaptées pour faire face aux situations d'urgence et d'incertitude.

Les professionnels qui excellent dans l'art de l'improvisation démontrent une combinaison de réactivité, de créativité et de prise de décision éclairée pour gérer efficacement les crises.

## Voici un aperçu des compétences clés et des stratégies utilisées dans l'improvisation en gestion de crise :

Compétences clés pour improviser en situation de crise :

- **Réactivité** : capacité à réagir rapidement et efficacement aux événements imprévus.
- **Créativité** : aptitude à trouver des solutions innovantes et originales face aux défis complexes.
- **Adaptabilité** : flexibilité pour s'ajuster aux changements rapides et aux nouvelles circonstances.
- **Communication efficace** : capacité à transmettre des informations claires et à coordonner les actions en temps réel.
- **Prise de décision rapide** : aptitude à prendre des décisions éclairées dans des délais contraints.

Stratégies et techniques d'improvisation en gestion de crise :

- **Anticipation** : prévoir les scénarios possibles et se préparer à réagir en conséquence.
- **Collaboration** : travailler en équipe pour mettre en commun les informations et les ressources et partager les responsabilités.
- **Flexibilité** : être prêt à ajuster les plans et les actions en fonction des changements survenus.
- **Gestion du stress** : maintenir son calme et sa concentration dans des situations tendues et critiques.
- **Apprentissage continu** : tirer des leçons des expériences passées pour améliorer sa capacité d'improvisation.

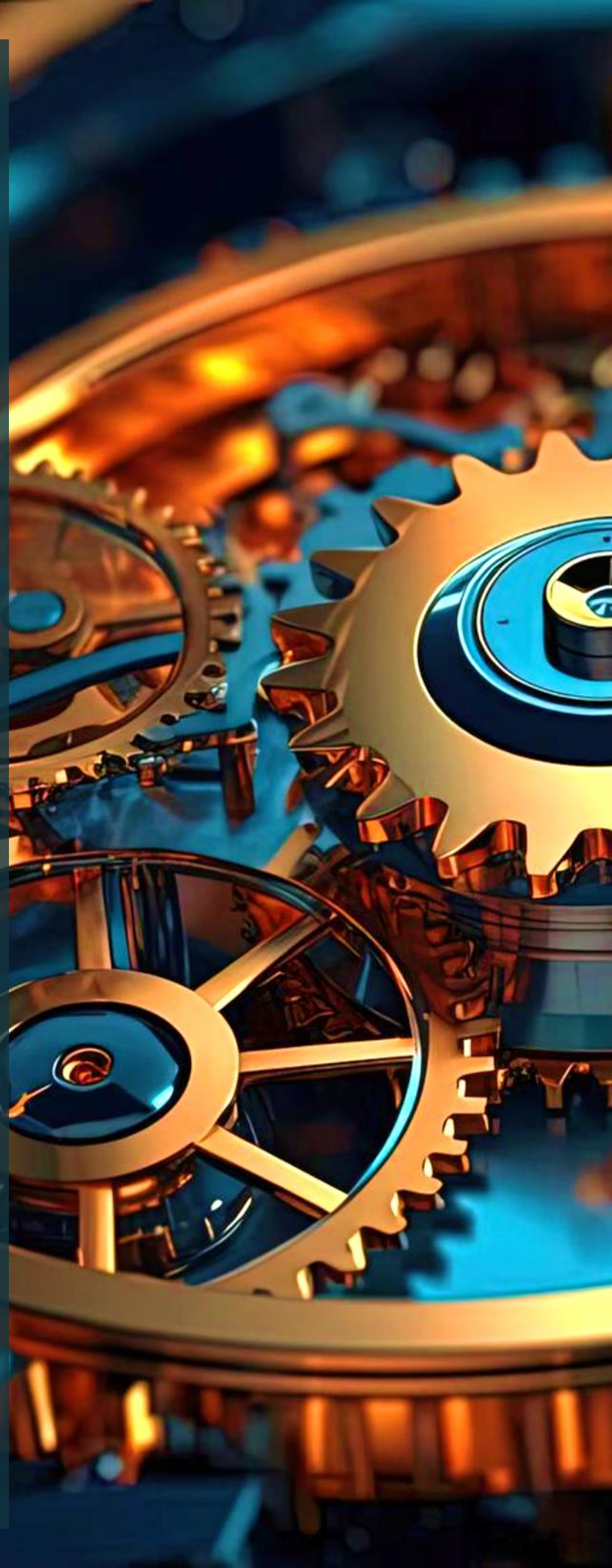
En développant les compétences et les stratégies décrites ci-dessus, les gestionnaires peuvent développer leur agilité mentale, leur capacité d'adaptation et leur aptitude à gérer efficacement les crises. L'improvisation en gestion de crise devient alors un atout stratégique majeur pour assurer la résilience organisationnelle face aux imprévus et aux situations critiques.


### Évolution de l'improvisation face aux défis contemporains

L'improvisation en gestion de crise a dû s'adapter et évoluer pour répondre aux nouveaux défis et enjeux rencontrés par les organisations dans un environnement en constante mutation. Face à des crises de plus en plus complexes et imprévisibles, l'improvisation se révèle être une compétence essentielle pour assurer la résilience et la survie des entreprises. Voici comment l'improvisation a évolué pour faire face aux défis contemporains :

Traumatisme organisationnel et nouvelles formes de crises :

- Le traumatisme organisationnel désigne les chocs majeurs qui perturbent profondément le fonctionnement d'une organisation, tels que les cyberattaques, les catastrophes naturelles ou les crises sanitaires. Ces événements inattendus exigent une capacité d'improvisation accrue pour gérer l'urgence et minimiser les impacts négatifs.
- Les organisations doivent être prêtes à faire face à des crises multiples et interconnectées, nécessitant une approche holistique de la gestion de crise et une collaboration étroite entre les différentes parties prenantes.





Adaptation des organisations à des situations inédites et à des urgences humanitaires :

- L'improvisation en gestion de crise s'étend désormais au-delà des frontières traditionnelles des entreprises pour inclure des situations humanitaires d'urgence, telles que les catastrophes naturelles, les conflits armés ou les pandémies.
- Les organisations doivent développer des capacités d'improvisation spécifiques pour répondre aux besoins humanitaires, mobiliser efficacement leurs ressources et coordonner leurs actions avec d'autres acteurs du secteur humanitaire.

Rôle de la gestion de crise dans la préparation à l'imprévu :

- Les organisations reconnaissent de plus en plus l'importance de la gestion proactive de crise pour anticiper les risques, renforcer leur résilience et améliorer leur capacité d'improvisation.
- La formation des équipes de gestion de crise, la simulation d'événements catastrophiques et la mise en place de plans d'urgence robustes sont autant de mesures essentielles pour préparer les organisations à faire face à l'imprévu.

La maîtrise de l'improvisation en gestion de crise est cruciale dans un monde où l'incertitude règne. Les professionnels, armés de connaissances solides et de compétences dynamiques, sont à même de réagir avec perspicacité face à l'adversité.

Cette aptitude évolutive est devenue une nécessité pour les entreprises qui cherchent à triompher face aux perturbations et aux crises humanitaires. La prévoyance, la résilience et la préparation sont les clés pour transformer les défis en opportunités de croissance durable.

Pour les leaders, prioriser l'amélioration des capacités d'improvisation et promouvoir une gestion des crises proactive est fondamental. En valorisant l'initiative, la créativité et l'esprit d'équipe, ils positionnent leur organisation pour réussir dans un environnement en mutation.



**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](http://www.crise-resilience.com)

## Pour aller plus loin, voici quelques références :

- Adrot, Anouck, et Garreau, Lionel, « [Interagir pour improviser en situation de crise : le cas de la canicule de 2003](#) », Revue française de gestion, no 203, avril 2010.
- Madiot, Laura, [Étude de l'improvisation dans le cadre d'une collaboration interprofessionnelle selon une perspective de sensemaking : le cas d'une équipe d'événementiel](#), Mémoire (M.A.), Université de Montréal.
- Olou, Prudence, [L'improvisation en gestion de projet : étude de quelques-uns de ses déterminants](#).
- Travaux de Weick sur l'improvisation en gestion de crise : [L'improvisation : pertinence du phénomène dans le comportement organisationnel](#).
- [Travaux de Cunha sur l'improvisation en gestion de crise](#) : SI & Management, Théories de l'improvisation organisationnelle : le bricolage, l'émergence, l'agilité... C. Ciborra, K. Weick.

# 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!



#4 – OCTOBRE 23



#3 – JUILLET 23



#2 – AVRIL 23



#1 – JANVIER 23

Abonnez-vous gratuitement sur [www.criseetresilience-magazine.com](http://www.criseetresilience-magazine.com)

## 🌟 Invitation à partager votre expertise !

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

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

### 👉 Comment participer ?

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

Nous avons hâte de découvrir vos perspectives uniques et vos approches novatrices pour renforcer la résilience et la gestion de crise dans le monde professionnel. Au plaisir de collaborer avec vous pour enrichir et éclairer notre communauté !

# 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](mailto:Info@crise-resilience.com)

# Risques climatiques, une approche globale devenue vitale

Aucune organisation, publique ou privée, ne sera à l'abri de l'augmentation de la fréquence et de l'intensité des aléas naturels, quelles que soient son activité et sa situation géographique.


En raison de leurs impacts potentiels majeurs sur toutes les catégories de risques accidentels, opérationnels, financiers et stratégiques, le traitement décloisonné (à 360°) du risque climatique n'est plus une option, mais une absolue nécessité.



par **Walter Munsch**



Associé en risk management  
Risk management & assurance  
Associate in risk management ARM (AMRAE The Institutes)  
Master 2 Management de l'assurance (ENASS)



**“D’ici 2050,  
les tempêtes,  
les inondations et  
les sécheresses  
pourraient entraîner  
des pertes de l’ordre de  
5 600 milliards \$ pour  
l’économie mondiale”**

*étude de GDH Group Limited*

Le dérèglement climatique est mondial, touchant indistinctement toutes les zones géographiques. Il est silencieux et hors de contrôle, les températures moyennes continuant de progresser inéluctablement.

L’année 2023 a enregistré 365 jours à +1 °C par rapport à la période préindustrielle (dont la moitié de l’année à plus de 1,5 °C), alors qu’en 2015 les signataires des accords de Paris s’étaient engagés à limiter le réchauffement à +2 °C d’ici 2100 – idéalement +1,5 °C. Le réchauffement climatique s’intensifie et s’accélère dans des proportions plus importantes que prévu.

En raison de la hausse des températures moyennes et de ses valeurs extrêmes, le réchauffement climatique a comme effet une augmentation de la fréquence et de l’intensité des catastrophes naturelles.

Chaleurs extrêmes en Asie, en Europe et en Amérique du Nord touchant au total 50 % de la population mondiale, feux de forêt devenus incontrôlables au Chili, au Canada, en Californie et en Australie, succession de tempêtes hivernales en France (Aline, puis Céline, puis Domingos), pluies diluviennes suivies d’inondations... Les dernières actualités ont été l’illustration des conséquences quotidiennes concrètes du changement climatique sur les populations et sur les biens.

En 2023, le montant des catastrophes naturelles est estimé à 260 milliards \$ au niveau mondial (Swiss Re), dont seulement 100 milliards \$ sont indemnisés par le marché de l’assurance, le champ assurantiel ne couvrant, en moyenne, que 30 % des risques.

### **Des conséquences importantes sur les systèmes assurantiers**

Plusieurs États ont d’ores et déjà mené des études prospectives afin d’anticiper les impacts du changement climatique sur leurs systèmes assurantiers.

En France, la CCR (Caisse centrale de réassurance) estime une augmentation de 40 % de la charge sinistre de catastrophes naturelles d’ici 2050, portée à 60 % en y ajoutant les variables liées à l’augmentation de la population et à la densité urbaine.

France Assureurs prévoit quant à elle que le coût des aléas naturels doublera tous les 30 ans et que le montant des sinistres dus aux événements naturels pourrait atteindre 143 milliards € en cumulé entre 2020 et 2050, soit une augmentation de 69 milliards € par rapport aux 30 dernières années.

Afin de faire face à cette augmentation attendue de la sinistralité en France, l’ACPR (Autorité de contrôle prudentiel et de résolution) envisage une hausse des primes d’assurance comprise entre 130 % et 200 % d’ici 2050.

Le taux de la cotisation de la surprime Cat Nat (catastrophe naturelle), obligatoirement incluse dans tous les contrats d’assurance « dommages aux biens », augmentera de 12 % à 20 % (soit +66 %) dès le 1er janvier 2025.

La surprime Cat Nat étant proportionnellement assise sur une assiette de primes qui augmente elle-même régulièrement chaque année, cette hausse sera mécaniquement très importante pour les professionnels et pour les entreprises.

Les conditions de souscription se sont d’ores et déjà durcies : augmentation des primes et des franchises, révision des textes de garanties, baisse des capacités. De plus, quelques assureurs se sont désengagés de leur marché en raison de la sinistralité enregistrée, d’une volatilité difficilement prévisible et du durcissement des conditions de réassurance.

Aujourd’hui, toute souscription est nécessairement associée à des mesures d’identification, de prévention et de réduction des risques.

En France, entre 1 000 et 2 000 communes n’auraient pas trouvé de solution d’assurance satisfaisante au 1er janvier 2024; aux États-Unis, 39 millions d’habitations sont menacées de perdre leur assurance en raison des événements climatiques extrêmes ayant notamment touché la Floride et la Californie.

## L'extension du risque climatique à la chaîne d'approvisionnement à ses interdépendances

Les effets d'une catastrophe climatique ne restent pas localisés à l'échelle d'un pays, ils se propagent et se diffusent dans le « village mondial » actuel où les processus commerciaux et industriels constituent une chaîne d'activités.

**En externalisant leurs productions et leurs approvisionnements, les entreprises ont également externalisé leurs risques et leurs revenus chez leurs fournisseurs, faisant évoluer le profil de leurs risques.**

Or un aléa climatique est susceptible d'impacter en profondeur toute la Chaîne d'approvisionnement d'une organisation et il peut aussi affecter l'ensemble d'une zone géographique, avec des conséquences directes ou indirectes sur les acteurs économiques d'une autre région du monde (l'effet « papillon »).

---

→ Le Canada (deuxième producteur mondial de graines de moutarde) a subi en 2021 une sécheresse particulièrement intense, faisant chuter sa production de graines de moutarde de 28 %. Cette pénurie a eu des impacts au niveau mondial, notamment en France, dont l'approvisionnement est lié à la production canadienne.

À cela s'est ajoutée une multiplication des ravageurs sur les exploitations locales due au réchauffement climatique, ce qui a accentué les difficultés de production.

**Conséquences : chute de la production nationale de moutarde de 50 %, hausse importante du prix de vente, pénurie.**

---

→ En 2011, les inondations en Thaïlande (deuxième producteur mondial de disques durs) ont arrêté la production de 15 000 usines de ce pays. La plupart des infrastructures clés (aéroports, routes, autoroutes) ont été paralysées, rendant impossible l'accès aux zones sinistrées, avec des conséquences pour toute l'industrie informatique mondiale.

**Conséquences : pénurie de composants, retards de lancement de produits, perte de parts de marché, etc.**







→ En France, sur les 800 entreprises qui ont été sinistrées par les récentes **inondations du Nord et du Pas de Calais**, 400 l'ont été directement... et 400 autres l'ont été indirectement : routes d'accès coupées ou impraticables, rendant impossibles les déplacements de leurs collaborateurs, les livraisons par leurs fournisseurs ou les livraisons d'une production ou d'un service à leurs clients.

**Conséquences : des pertes importantes de chiffres d'affaires non indemnisées, par leurs assurances, car ces entreprises n'ont pas subi de dommages directs.**

---

Un contrat d'assurance dommages se limitera à l'indemnisation des dégâts directs subis par son assuré et, parfois, aux conséquences financières liées à un dommage touchant un fournisseur/client identifié (si souscription d'une garantie contre la carence des fournisseurs/clients).

Or il est indispensable de prendre aussi en compte les conséquences d'une interruption d'approvisionnement de fournisseurs non identifiés et la complexité des interdépendances d'une Chaîne d'approvisionnement.

Les nouvelles solutions d'assurance dites « paramétriques » peuvent représenter une solution pour certaines situations, mais conçues sur mesure, elles restent coûteuses, car peu mutualisées.

L'assurance prend en compte les conséquences immédiates d'un sinistre, mais ne peut être une solution pour indemniser l'ensemble des impacts à moyen et à long terme (pénuries, volatilité des matières premières, pertes de parts de marché et de capitalisation boursière, etc.).

Certains enjeux financiers majeurs consécutifs à un aléa climatique ne peuvent faire l'objet d'un transfert à l'assurance et ils doivent être traités différemment.

## Réchauffement climatique : risques géopolitiques et risques sanitaires

L'insécurité alimentaire due au changement climatique et les pénuries en eau seront les causes de violences et de désordres.

Le GIEC (Groupe d'experts intergouvernemental sur l'évolution du climat) a évoqué la situation de forte compétition entre États et la possibilité de conflits pour l'accès aux ressources vitales dans son scénario Shared Socioeconomic Pathways (SSP) lié à un réchauffement climatique RCP 8,5 (hausse des températures à + 4 °C).

En 2010, les récoltes de blé russe ont été fortement impactées par des chaleurs extrêmes et des incendies. La production et les exportations ont baissé de 30 %, créant une pénurie, et les cours ont augmenté de 60 %. Le blé est un produit de première nécessité au Maghreb, cette situation a mis le feu aux poudres et a contribué au déclenchement du Printemps arabe.

**Au total, 33 millions de personnes  
se sont déplacées dans la continuité  
de catastrophes naturelles.**

À l'horizon 2050, 216 millions d'individus seraient concernés par une migration d'origine climatique.


L'Asie, qui a des échanges commerciaux importants avec les pays occidentaux, en serait particulièrement impactée avec comme conséquence des risques géopolitiques accrus.

L'eau, ressource souvent transfrontalière, est d'ores et déjà l'objet de vives tensions entre États, et son accès est l'objet de contentieux. Dernièrement, la France a demandé à la Suisse l'augmentation du débit du Rhône (qui alimente en eau quatre de ses centrales nucléaires), son niveau ayant beaucoup baissé pendant la période estivale.

À la suite d'une période de fortes chaleurs, le Portugal a reproché à l'Espagne de trop puiser dans le fleuve Tage pour alimenter sa zone de production agricole en Andalousie.

La baisse du niveau de l'eau à la suite de sécheresses sera la cause de désordres sur les chaînes d'approvisionnement des entreprises utilisant les voies maritimes comme mode de transport. L'impossibilité de naviguer sur le Rhin en 2022 a eu des impacts directs sur les entreprises françaises et allemandes ainsi que sur la production d'électricité des usines hydroélectriques.

Le ralentissement de la navigation sur le canal de Panama en 2023 (où transite 5 % du trafic mondial) en est aussi l'illustration.



**À l'horizon 2050,  
216 millions d'individus  
seraient concernés par une  
migration d'origine  
climatique.**



## **Les pandémies risquent de devenir plus fréquentes.**

La perte de biodiversité et les déforestations sont à l'origine d'une progression des maladies infectieuses à l'échelle mondiale, les animaux venant au contact de l'humain afin de trouver un habitat plus viable. Ce partage viral (appelé zoonose) entre l'humain et des espèces sauvages qui étaient auparavant isolées géographiquement est un facteur important de risque.

De plus, la hausse des températures favorise le développement d'insectes porteurs de maladies, tel le moustique, qui transmet le virus Chikungunya et la dengue à l'homme.

La fonte des glaces, mais aussi l'exploitation de zones aujourd'hui accessibles en raison du réchauffement climatique (Sibérie), pourrait libérer des virus et des bactéries inconnus qui étaient emprisonnés dans le pergélisol depuis des millénaires.

Les fortes canicules favorisent une élévation importante de la température de l'homme au-dessus des valeurs normales, l'hyperthermie, pouvant entraîner une surmortalité.

On estime que la canicule européenne de l'été 2022 a causé plus de 60 000 décès, chiffre qui pourrait être multiplié par 5 à l'avenir dans le cas où les températures moyennes augmenteraient de +2 °C.

Les fortes chaleurs pourraient aussi entraîner des ruptures importantes de production pour les activités menées à l'extérieur (construction, entretien d'infrastructures), les ouvriers ne pouvant travailler dans des situations acceptables pour leur santé.

Les risques psychosociaux des salariés doivent aussi être pris en compte, car ils peuvent être confrontés à des stress post-traumatiques importants sur leur lieu de travail lors d'inondations, de tempêtes extrêmes, etc.

Les risques liés à l'écoanxiété (perte de sens au travail, désengagement, difficulté de recrutement) en relation avec le réchauffement climatique et les crises environnementales sont aussi en augmentation.

## Climat et responsabilité sociétale : risque de transition et devoir de vigilance

Le simple examen des dommages que la nature peut causer à l'entreprise ne sera plus suffisant.

Sous pression réglementaire, une entreprise devra également mener une analyse plus globale et communiquer sur un spectre élargi :

- Comment s'adapte-t-elle à l'évolution de son environnement et à l'économie verte (risque de transition)?
- Comment ses activités peuvent-elles contribuer aux objectifs de développement durable?
- Quels sont les dommages qu'elle peut causer à la nature?

Le risque de transition, en lien avec le risque climatique, inclut les risques liés au processus d'adaptation de l'entreprise vers une économie à faibles émissions de carbone.

Par exemple, une organisation ayant un impact négatif sur la biodiversité s'exposera à l'établissement de nouvelles réglementations qui l'obligeront à modifier son modèle d'affaires ou ses produits, avec comme risque une perte de ses consommateurs.

Cette situation pourrait exposer défavorablement les acteurs de son financement (banques, assureurs, investisseurs), et c'est pourquoi la notion de durabilité doit être intégrée dans la gestion des risques.

La CSRD (Corporate Sustainability Reporting Directive), une directive européenne, cadre cette exigence de transparence en imposant aux entreprises de présenter un rapport de durabilité extrafinancier sur de nombreux critères ESG (environnementaux, sociaux et de gouvernance) et de faire l'analyse d'une double matérialité :

- la matérialité financière, par la prise en compte des impacts positifs et négatifs des enjeux de durabilité (risque de transition) sur les performances financières de l'entreprise;
- la matérialité d'impact, par la prise en compte des impacts positifs et négatifs de l'entreprise sur son environnement économique, social et naturel (changement climatique, biodiversité, etc.).

Son objet est de communiquer aux parties prenantes toutes les données leur permettant d'analyser la stratégie de l'entreprise sur le traitement de ses risques physiques (quels sont les plans d'adaptation mis en place?) et de ses risques de transition à moyen ou long terme (le business model est-il adapté?).

Par sa vision holistique sur les enjeux et les impacts, la CSRD oblige tous les acteurs d'une entreprise à se mobiliser et à travailler en étroite collaboration : gestionnaire de risque, responsable RSE (Responsabilité Sociétale des Entreprises), direction financière, métiers opérationnels. En cela, elle plaide pour une approche décloisonnée du risque climatique.

Applicable dès 2024 aux grands groupes (plus de 5 000 salariés), cette directive européenne se généralisera jusqu'en 2027 aux PME de plus de 250 salariés (50 000 entreprises) et, en 2028, aux entreprises extraeuropéennes réalisant un chiffre d'affaires de plus de 150 millions € au sein des pays membres de l'Union européenne.





Une deuxième directive européenne, la CS3D (Corporate Sustainability Due Diligence Directive), est en cours de discussion.

Son objet est d'imposer aux entreprises de plus de 500 salariés et de plus de 150 millions € de CA (hors secteur financier) un devoir de vigilance sur l'ensemble de leur chaîne de valeur, avec notamment la surveillance des impacts négatifs de leurs activités sur la pollution, la déforestation, la consommation excessive d'eau et les dommages causés aux écosystèmes.

En France, une loi adoptée en 2017 impose déjà un plan de vigilance aux sociétés mères et aux entreprises donneuses d'ordre de plus de 5 000 salariés.

Étendu à leurs sous-traitants et fournisseurs, ce plan de vigilance inclut l'identification des risques ainsi que la mise en œuvre de mesures de prévention et de mécanismes d'alerte pour toute atteinte aux droits humains, à la santé et à la sécurité des personnes et à l'environnement.

Les entreprises concernées s'exposent à des actions en réparation de préjudices et à des sanctions s'il y a non-respect de cette obligation.

Les risques liés à la stratégie ESG sont à présent de plus en plus élevés.

En relation avec la stratégie climatique de l'entreprise et intégrés à la gestion globale de ses risques, ils incluent aussi le risque de financement – impossibilité de trouver des capitaux auprès d'investisseurs – et le risque de réputation.

**“En relation avec sa stratégie climatique, toute entreprise peut être critiquée pour ses pratiques, avec comme conséquences le boycottage de ses produits, une mise en cause sur les réseaux sociaux, une baisse de ses ventes et une dégradation durable de son image de marque.”**

*Walter Munsch*

**“Cela ne sera pas un bang,  
mais un long  
gémissement.”**

**Jean Pierre DUPUY,**

*Annales des Mines – Responsabilité et Environnement - 2022*

### **Anticiper et se préparer au monde de demain**

L'ajout de CO<sub>2</sub> à l'atmosphère augmente les températures. Néanmoins, ces émissions continuent de progresser inexorablement : +1,1 % en 2023 (36,8 milliards de tonnes de dioxyde de carbone émises), alors qu'il faudrait les réduire de 42 % d'ici la fin de la décennie pour limiter le réchauffement à +1,5 °C.

**Si les émissions se poursuivent à ce rythme, la concentration de CO<sub>2</sub> pourrait monter à 600 ou à 800 ppm (parties par million), alors qu'elle est actuellement à 420 ppm et qu'elle augmente 3 fois plus rapidement qu'il y a 50 ans.**

Le temps de réaction de la Terre aux efforts de réduction des gaz à effet de serre (GES) n'est pas immédiat (« inertie climatique »), car leur durée de vie est variable :

- dioxyde de carbone (CO<sub>2</sub>) – 100 ans;
- méthane (CH<sub>4</sub>) – 12 ans;
- oxyde nitreux (N<sub>2</sub>O) – 114 ans;
- hydrocarbures (CFC et HCFC) – 3 200 ans.

Les effets d'une hausse ou d'une baisse des émissions des GES (gaz à effet de serre) ne se font ressentir qu'après 20 à 40 ans, et les gaz déjà présents vont donc continuer de réchauffer la planète.

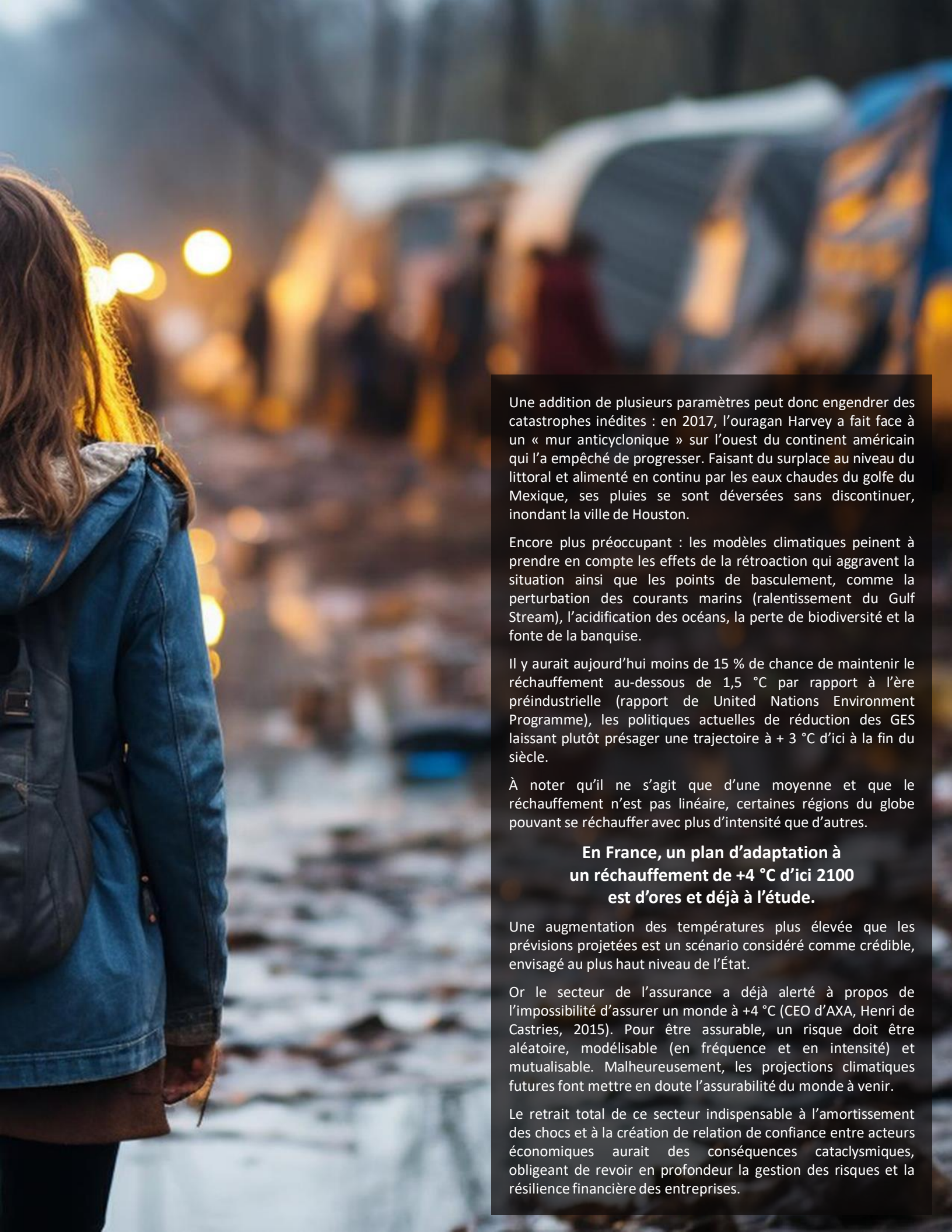
Le rejet du CO<sub>2</sub> n'est pas le seul paramètre à prendre en compte, car il existe une interconnexion entre le climat, les écosystèmes et la société humaine. La biomasse et les océans (qui captent 50 % des émissions) sont essentiels :

**6 limites planétaires sur 9 ont déjà été dépassées, avec comme conséquences des dommages irréversibles qui aggraveront les conséquences du réchauffement.**

Un aléa climatique peut déclencher un phénomène qui s'autoalimente et qui s'amplifie de lui-même par la conjonction de différentes évolutions simultanées. Les exemples de « rétroaction » sont nombreux :

- Des feux de tourbe se propagent par le sol et, en libérant des gaz, vont accroître le réchauffement climatique.
- L'accumulation de la chaleur de l'océan entraîne une dilatation, responsable de la montée des mers.
- Des feux de forêt intenses créent la formation de nuages appelés pyrocumulus qui, se chargeant d'électricité, déclenchent foudre et incendies.





Une addition de plusieurs paramètres peut donc engendrer des catastrophes inédites : en 2017, l'ouragan Harvey a fait face à un « mur anticyclonique » sur l'ouest du continent américain qui l'a empêché de progresser. Faisant du surplace au niveau du littoral et alimenté en continu par les eaux chaudes du golfe du Mexique, ses pluies se sont déversées sans discontinuer, inondant la ville de Houston.

Encore plus préoccupant : les modèles climatiques peinent à prendre en compte les effets de la rétroaction qui aggravent la situation ainsi que les points de basculement, comme la perturbation des courants marins (ralentissement du Gulf Stream), l'acidification des océans, la perte de biodiversité et la fonte de la banquise.

Il y aurait aujourd'hui moins de 15 % de chance de maintenir le réchauffement au-dessous de 1,5 °C par rapport à l'ère préindustrielle (rapport de United Nations Environment Programme), les politiques actuelles de réduction des GES laissant plutôt présager une trajectoire à + 3 °C d'ici à la fin du siècle.

À noter qu'il ne s'agit que d'une moyenne et que le réchauffement n'est pas linéaire, certaines régions du globe pouvant se réchauffer avec plus d'intensité que d'autres.

**En France, un plan d'adaptation à un réchauffement de +4 °C d'ici 2100 est d'ores et déjà à l'étude.**

Une augmentation des températures plus élevée que les prévisions projetées est un scénario considéré comme crédible, envisagé au plus haut niveau de l'État.

Or le secteur de l'assurance a déjà alerté à propos de l'impossibilité d'assurer un monde à +4 °C (CEO d'AXA, Henri de Castries, 2015). Pour être assurable, un risque doit être aléatoire, modélisable (en fréquence et en intensité) et mutualisable. Malheureusement, les projections climatiques futures font mettre en doute l'assurabilité du monde à venir.

Le retrait total de ce secteur indispensable à l'amortissement des chocs et à la création de relation de confiance entre acteurs économiques aurait des conséquences cataclysmiques, obligeant de revoir en profondeur la gestion des risques et la résilience financière des entreprises.

Le dérèglement climatique est porteur de risques systémiques par son incidence directe sur les activités humaines, les activités urbaines et les systèmes socio-économiques.

Mondial, mais aussi local, ce dérèglement a des effets qui sont en interconnexion avec toutes les typologies des risques des entreprises.

Les défis à relever sont nombreux :

- sinistralité Cat Nat,
- menace d'inassurabilité,
- complexité des chaînes de valeur dans une économie mondialisée,
- pression réglementaire liée au rôle sociétal de l'entreprise et à sa trajectoire climat et projections climatiques alarmantes, car l'atténuation des GES ne portera ses fruits que dans plusieurs décennies.

Les catastrophes climatiques passées ont démontré combien l'anticipation (ex ante) associée à une gestion de crise appropriée (ex post) pouvait avoir une incidence directe sur la résilience et la performance des entreprises.

C'est pourquoi elles devraient agir dès à présent en identifiant dans leur cartographie tous les risques liés au climat afin de les intégrer aux risques existants, tout en mettant conjointement en place des mesures d'adaptation.

Cette analyse à 360° exige transversalité et décloisonnement de leurs différents départements, un pilotage de chaque instant et, en raison de la nature systémique du risque climatique, une gouvernance au plus haut niveau.

En associant cette approche holistique à ses décisions stratégiques, l'entreprise se donnerait les moyens et les pouvoirs de prendre toutes les mesures de prévention nécessaires au maintien de son activité, de ses parts de marché, de sa compétitivité et de sa performance, quelles qu'en soient les circonstances.

**Au regard de la situation actuelle et des enjeux du futur, la gouvernance du risque climatique n'est plus une option, mais une absolue nécessité.**

 **Walter Munsch**

25 ans d'expérience au sein de cabinets de courtage en assurances des risques d'entreprise (PME, ETI et grands comptes)

Conseil en gestion des risques : identification, analyse, traitement et transfert au marché de l'assurance

Accompagnement en prévention et en réduction de risques

Formateur - conférencier

[www.linkedin.com/in/walter-munsch/](https://www.linkedin.com/in/walter-munsch/)

## ÉTAPES CLÉS, CONSEILS ET ASTUCES

### Analyse à 360°

#### du risque climatique :

Le risque climatique est systémique et stratégique. Son analyse via la réalisation d'une cartographie dédiée nécessite de fédérer différents métiers : gestion des risques, RSE, finance, production, service juridique, RH, conformité, achats, etc., et de partager avec le COMEX (Comité Exécutif).

Il est recommandé d'identifier au préalable quels sont les acteurs à inclure dans cette démarche et d'adopter une méthodologie de conduite de projet agile :

- Identifier les aléas climatiques vecteurs de risques pouvant impacter les activités de l'entreprise et les mettre en relation avec ses enjeux prioritaires.
- Mener en parallèle une démarche prospective afin d'anticiper les conséquences futures du réchauffement climatique sur l'organisation via des données géoclimatiques.
- Identifier les actifs critiques (bâtiments, usines, etc.) et les zones géographiques concernées et croiser les données climatiques avec la localisation des actifs retenus.
- Analyser les expositions et les vulnérabilités en intégrant les tendances climatiques futures.
- Appréhender la globalité de la Chaîne d'approvisionnement (moyens de transport, zones géographiques, saisonnalité) et ses expositions aux aléas climatiques.
- Analyser sa chaîne de valeur et son business model sous l'angle des risques et des opportunités liés à la transition sur les sujets ESG.
- Intégrer le risque climatique dans les risques existants préalablement identifiés.
- Traiter les vulnérabilités par des mesures d'adaptation et travailler à la réduction du risque résiduel.
- Élaborer un plan de continuité d'activité (PCA).
- Déployer un plan d'action avec animation régulière.



## Conseils sur le traitement des risques climatiques physiques

Avoir une approche systémique afin de ne pas se limiter à la simple matérialité d'un actif, et prendre aussi en compte son environnement :

- Quelle est son accessibilité (routes, port, etc.)?
- Quelle est sa dépendance aux télécoms, à l'électricité, à l'alimentation en eau? Par quels moyens est-il approvisionné en matières premières/produits finis?
- Quels sont les équipements indispensables à son activité?
- Quelles sont ses interdépendances avec les autres sites de l'entreprise?
- Si le site est basé à l'étranger, quelles sont les relations avec les autorités locales et les moyens mis à disposition en cas de destruction des infrastructures publiques?

## Conseils sur le traitement des risques climatiques de la Chaîne d'approvisionnement

Aller plus en profondeur, ne pas se limiter au rang 1. Se poser des questions :

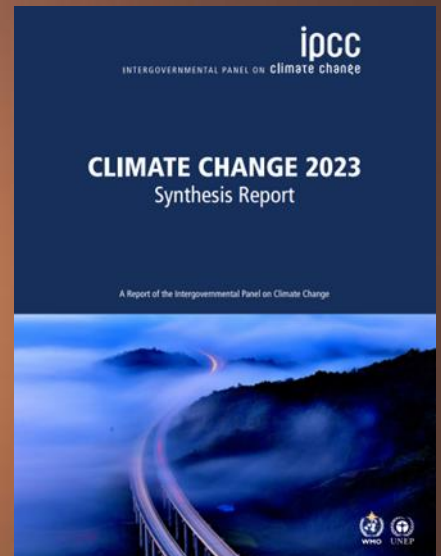
- Où se situe la dépendance de mes profits? (Un composant peut avoir un prix d'achat minime, mais participer à la réalisation d'un CA important.)
- Qui sont mes fournisseurs critiques?
  - Apportent-ils une forte valeur ajoutée?
  - Quelles sont leurs sources d'approvisionnement?
  - Quelle est leur exposition aux risques climatiques?
  - Ont-ils mis en place un PCA?
- Existe-t-il des solutions de transfert de production?
- Quelles sont les actions à mener afin d'améliorer la robustesse (redondance de certains moyens stratégiques), la flexibilité (transfert d'un site à un autre), la visibilité (alerte et action rapide en cas de rupture) et la collaboration (échange d'informations stratégiques pour une réaction optimale)?

## Conseils sur le traitement du risque de transition et du devoir de vigilance

Se poser les questions suivantes :

- Quels sont les moyens mis en œuvre par mon entreprise pour atténuer le réchauffement climatique?
- Quelle est ma stratégie en matière de climat?
- Quels sont les impacts de mon business model pour les parties prenantes (citoyens, consommateurs, salariés, écosystème, institutions, planète)?
- Quelle est ma trajectoire carbone?
- Mes fournisseurs ont-ils un impact sur l'environnement (déforestation, atteinte à la biodiversité)?
- Quelle est mon utilisation des ressources et des déchets?
- Quels sont les risques et les opportunités liés à la transition (risques : réputation, risque de financement, business model inadapté à la préservation de l'environnement, etc.; opportunités : différenciation commerciale, économies énergétiques, marque employeur valorisée, etc.).

# En savoir plus sur les risques liés au climat



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

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



Téléchargez gratuitement  
5 idées de scénarios de  
gestion de crise

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

**Attention le nombre de places est limité!**

[crise-resilience.com/simulation](https://crise-resilience.com/simulation)

# TÉLÉCHARGER GRATUITEMENT 15 AFFICHES DE SENSIBILISATION




A TÉLÉCHARGER SUR [WWW.CRISE-RESILIENCE.COM](http://WWW.CRISE-RESILIENCE.COM)

Télécharger ici

# Le coordinateur de crise, le casting stratégique!

Zoom sur le coordinateur de la cellule de crise, du profil à l'action, pour vous permettre de faire le premier vrai bon choix dans l'optimisation de vos processus de crise : choisir la personne qui va l'animer.



par Anne-Gervaise Vendange 

Cofondatrice et présidente de In Cognita  
Profileuse et systémicienne



Vous le savez, si vous vous intéressez à la crise de près ou de loin, le coordinateur de crise est un poste essentiel à pourvoir pour traverser la tempête dans des conditions optimales. Oui, mais voilà, quand j'interviens dans les entreprises, et spécialement dans celles qui n'étaient pas préparées à faire face à l'inattendu qui s'abat sur elles, je vois trop souvent des coordinateurs qui n'ont pas le bon profil ou qui ne sont pas là pour les bonnes raisons.

Il est pourtant primordial de saisir toute la profondeur de ce poste qui peut faire passer une cellule de crise d'une vente à la criée à 6 h du matin à un bras armé redoutablement efficace.

### Une place primordiale

Le travail du coordinateur consiste avant tout à gérer la cellule et à en être le garant structurel.

Cela implique d'avoir évidemment bien compris les tenants et les aboutissants d'une gestion de crise, mais aussi de bien connaître l'organisation dans laquelle il opère, ce qui est déjà un défi en soi!

Il m'est arrivé de voir des coordinateurs fraîchement arrivés dans l'entreprise, comme si c'était un poste que tout le monde pouvait honorer, et que, pour libérer les plus anciens, on mettait, comme dans l'armée, le dernier arrivé à des tâches subalternes.

Or la coordination de crise est tout sauf une tâche subalterne ou annexe. Et j'espère qu'après la lecture de ces quelques lignes, cela sera devenu une évidence pour vous aussi.

### Recherché : couteau suisse avec du leadership

À ce poste, on organise la circulation de l'information, y compris avec les autres cellules. On met aussi en musique les très cruciaux « points de situation », qui centralisent les faits et les actions afin que tout le monde possède le même niveau d'information, élément essentiel à la bonne gestion d'une crise.

Pour tout cela, le coordinateur devient le point central à qui tout le monde se réfère. Il est donc important qu'il possède l'assise et la légitimité nécessaire aux yeux des équipes afin de pouvoir se faire entendre facilement.

Il faudra choisir un profil avec un bon sens de la synthèse capable de prioriser les éléments qui viennent à lui, mais aussi s'assurer que cette personne saura déléguer. En effet, la personne qui tient le rôle de coordinateur distribue la parole, mais attribue aussi les tâches.

Gardez cela à l'esprit : si le coordinateur est en train de faire quelque chose, c'est qu'il n'est pas à sa place. Son obsession doit être de déléguer afin de continuer à être disponible à sa tâche essentielle au sein de la cellule : l'organiser.

**“Gardez cela à l'esprit : si le coordinateur est en train de faire quelque chose, c'est qu'il n'est pas à sa place.”**

*Anne-Gervaise Vendange*

Il collecte les problèmes, organise leur résolution et attribue pour cela des tâches en prenant en compte l'expertise et la disponibilité de chacun. Évidemment, afin de pouvoir se donner totalement à cette charge, il ne doit pas être un expert métier de la crise en cours.

Il est important que le coordinateur soit doté d'une certaine intelligence émotionnelle et relationnelle, mais qu'il sache aussi s'imposer et qu'il ne craigne pas le conflit.

En effet, il peut être amené, au cours de sa mission, à questionner les experts métiers, et même, parfois, à recadrer les décideurs afin de leur permettre de profiter de la structure de la cellule à son plein potentiel pour prendre les meilleures décisions.

Une très bonne stabilité émotionnelle sera aussi un vrai plus. Une cellule de crise vit des hauts, des bas et des flots d'émotions parfaitement normaux. Il est important que le coordinateur puisse supporter une certaine pression afin de conserver un recul sur la situation et sur le cheminement des êtres humains qui la composent.

Une autre de ses tâches est de mettre en place l'organisation spatiale et logistique de la cellule de crise et de ses satellites. Il doit veiller à ce que la cellule ne manque de rien : nourriture, boissons, papier, affichage, subsidiarité des postes. Il doit aussi porter attention à la fatigue de chacun.

Ces compétences, qui sont rarement inscrites dans un CV lors de l'embauche, sont pourtant tellement importantes pour permettre à une cellule et à ses experts de durer dans le temps.

Et, pour finir, le coordinateur organise les retours d'expérience, partie intégrante d'une bonne gestion de crise et un des temps forts d'un management réussi.

La coordination est une tâche vitale à la cellule de crise. Le choix de son coordinateur ne doit rien laisser au hasard.

Bien sûr, ce poste nécessite de l'expérience et du savoir-faire, mais plus que cela encore, il nécessite un grand savoir-être permettant de mettre du liant et de la structure au sein d'une cellule de crise malmenée par les événements et les émotions générées par la crise.

Faire ce choix de manière éclairé peut avoir une réelle incidence sur l'efficacité de votre gestion de crise et sur ses conséquences.

### **Anne-Gervaise Vendange**



Experte en profilage, en influence, en gestion et en communication de crise. Co-fondatrice de In-Cognita

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

Depuis 2020, In Cognita intervient et forme dans les domaines de la gestion de crise, de la communication de crise et de la négociation à fort enjeu afin d'aider les décideurs à faire face à l'inattendu, qui parfois les dépasse.

<https://in-cognita-corp.com/>



## Pour aller plus loin, voici quelques références :

### Carte d'identité du coordinateur de crise :

- Il connaît bien l'organisation et les gens qui la composent.
- Il est légitimé aux yeux de ses pairs.
- Il fait preuve de leadership, mais aussi d'assertivité.
- Il est équipé d'intelligence relationnelle et émotionnelle.
- Il a le sens de la synthèse.
- Il a une très bonne stabilité émotionnelle.
- Il ne craint pas le conflit.
- Il n'est pas un expert métier (de la crise en cours).
- Il lui faut évidemment de la subsidiarité; il vous faudra donc trouver à minima deux de ces pépites 😊 .

### Tâches au sein de la cellule de crise :

- Il anime la cellule.
- Il organise et anime les points de situation.
- Il distribue la parole.
- Il questionne les experts métiers.
- Il collecte les problèmes et organise leur résolution.
- Il attribue des tâches.
- Il organise la circulation de l'information, y compris avec les autres cellules.
- Il doit, parfois, recadrer les décisionnaires.
- Il met en place l'organisation spatiale et logistique de la cellule de crise et de ses satellites.
- Il organise les retours d'expérience.

## Lire les autres articles d'Anne-Gervaise Vendange

Cliquer sur  
l'image



# L'espionnage industriel dans une PME? Ce n'est pas du cinéma!

« Chez nous? Au Québec?  
Dans nos PME?

Ben voyons, l'espionnage  
industriel, ça ne frappe  
que les grands groupes  
et les États! »

Si c'est ce que vous  
pensez, alors c'est vous  
qui êtes dans la fiction, et  
la réalité va vous  
stupéfier.

par Philippe Chevalier



Détective en affaires d'entreprise : enquêtes de déloyauté, fraudes, enquêtes sur des associés, contre-espionnage industriel.

Cyberenquête de réputation augmentée par l'IA.







“ Remplaçons le mot  
« espionnage »  
par « **déloyauté** »  
et soudainement,  
cela paraît plus proche  
et plus réel. ”

*Philippe Chevalier*

Stéphane ne comprend pas. Son entreprise métallurgique, qui fabrique des plateformes modulaires innovantes et réputées pour des camions semi-remorques, perd tous les appels d'offres depuis un an.

Et aujourd'hui, c'est le contrat TYT qui lui échappe! LE contrat de l'année, négocié depuis 2022.

Stéphane ne pouvait pas penser à de l'espionnage industriel. Pourquoi l'aurait-il fait? Il n'est pas dans l'industrie de l'armement, ni dans l'informatique quantique, ni dans l'aéronautique ou le pharmaceutique.

Stéphane est dans le métal! Des systèmes de remorques de camions, 50 employés. Il vend au Canada et aux États-Unis, un peu au Mexique. Stéphane, ce n'est pas dans l'univers habituel de l'espionnage, n'est-ce pas?

Et pourtant, avant de vous révéler la fin de sa mésaventure, voici une introduction à la réalité du monde de l'espionnage industriel.

### Comment compromettre un employé clé afin qu'il livre des secrets stratégiques? C'est le MICE :

- **Money** : vulnérabilité financière en raison d'un divorce, d'un prêt hypothécaire alourdi, de changements de vie, etc.
- **Idéologie** : vulnérabilité à l'influence d'un groupe militant.
- **Chantage** : vulnérabilité... eh bien, le mot dit tout.
- **Ego** : vulnérabilité de l'employé incompris qui cherche sa revanche.

**Et ce n'est pas de la fiction,  
car parmi vos compétiteurs se trouvent  
des personnes très déterminées.**

### Voici quatre exemples issus de nos enquêtes :

- **M - Money** : un agent courtier en fret aérien et maritime, surendetté (casino), qui transmet les dossiers clients au concurrent en échange d'argent.
- **I - Idéologie** : une employée (militante de la cause animale) travaillant pour un fabricant de vêtements (quelques fibres animales) qui transmet tous les plans stratégiques au compétiteur qui, lui, assurait n'utiliser que des fibres synthétiques.
- **C - Chantage** : ce super vendeur d'une *start-up* en TI qui s'est « laissé aller » un soir à Las Vegas après un salon d'exposition et, malheureusement, un concurrent a « documenté sa nuit de détente ». « Eh bien non, Jimmy, la majorité n'est pas partout à 18 ans aux États-Unis. Es-tu sûr que la fille avait bien 21 ans? Les photos... on va les garder un petit moment. »
- **E - Ego** : et c'est ici que nous retrouvons l'entreprise de Stéphane et ce superviseur de production, 22 ans d'ancienneté, qui connaît tous les secrets de fabrication dans l'usine de Stéphane.

Le pilier de l'entreprise, qui n'a jamais accepté l'arrogance des deux jeunes ingénieurs stagiaires devenus ses supérieurs. Il s'est laissé facilement convaincre par le concurrent ontarien de lui transférer à l'avance les réponses aux appels d'offres. Pas besoin de le payer, il suffisait de le flatter.

L'espionnage industriel est un terme mal compris. Il semble associé à ce qui n'arrive qu'aux autres ou à des histoires complexes concernant les offensives économiques d'un pays lointain.

Alors, remplaçons le mot « espionnage » par « déloyauté » et, soudainement, cela paraît plus proche et plus réel.

## Le dénouement?

Il passe par la suppression du déni. L'espionnage industriel ou l'espionnage en affaires est monnaie courante. Nos derniers clients à ce sujet sont des PME dans le secteur de la santé – pas même des industries, mais des PME de service.

Voici l'acronyme **PADA** pour répondre à **MICE** :

- **Perception** : si votre concurrent semble connaître vos prix, vos clients, vos projets... c'est qu'il les connaît.
- **Analyse** : est-ce qu'il y a d'autres explications que la déloyauté?
- **Décision** : faites une enquête, idéalement menée par une ressource externe, car la cyberenquête ou simplement la filature, la contre-manipulation, les entrevues et les interrogatoires, c'est technique et c'est encadré légalement. Seule une agence d'enquête sera à la fois efficace et légale.
- **Action** : si des faits sont établis et prouvés par une enquête, des avocats et des relationnistes sont nécessaires pour non seulement faire face à la crise, mais aussi pour la transformer en victoire, car l'espionnage industriel, c'est comme l'amour, ce n'est pas obligé de finir mal.

Je ne peux pas vous révéler le nom de l'entreprise de Stéphane (j'ai modifié un peu son secteur d'activité pour l'article), mais vous devinez que son PADA a fonctionné et qu'une enquête lui a été fort utile.

L'acronyme MICE vient du monde du renseignement et se réfère aux techniques de manipulation d'une source. L'acronyme PADA vient de la police (Sûreté du Québec) et se réfère à son protocole d'intervention.

Et, en effet, notre agence regroupe des retraités de ces deux services avec de jeunes *hackers* éthiques, cyberdétectives (et quelques IA spécialisées). Tous sont familiers avec les crises, alors ils savent aussi que le pire n'est jamais certain... mais que cela vaut la peine de vérifier et d'enquêter.

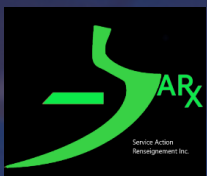
L'espionnage industriel ou en affaires semble souvent associé aux cybermenaces, aux pirates, et c'est vrai jusqu'à un certain point. C'est d'ailleurs pour cette raison que nous employons des cyberenquêteurs.

Mais le mot clé demeure la vulnérabilité humaine, qui permet la manipulation. Cela reste un facteur humain, et c'est sans doute ce qui rapproche l'espionnage en affaires de l'espionnage étatique.

James Bond ne franchira pas les portes de votre entreprise, et, s'il le fait, il ne sera pas dangereux car, lui, au moins, il se nomme spontanément : « My name is Bond. »

Donc, la réalité est effectivement plus sournoise que la fiction.

### Philippe Chevalier



Sarx inc. est une agence de détectives privés autorisée exerçant ses activités depuis 10 ans pour les entreprises.

Sarx enquête au Canada, aux États-Unis, en Europe, aux Émirats arabes unis, dans les Caraïbes et à travers le monde avec des techniques de cyberenquête et d'OSINT augmentées par l'IA.

<https://www.sarx.net/>

## Deux réflexions pour être moins vulnérable

1 - La première est vraiment simple et ne demande aucun investissement, ni en matériel ni en temps.

- Pour protéger vos informations stratégiques, demandez-vous quelle est la distinction utile entre le droit de savoir et le besoin de savoir. Bien des affaires d'espionnage ou de déloyauté ont causé du dégât, car la mauvaise personne avait accès à la bonne information et a pu la faire sortir de l'entreprise.
- C'est un peu contre-intuitif quand tout le monde vous dit de ne pas travailler en vase clos, mais prenons le cas de l'entreprise Dyson, qui avait le prototype de la voiture électrique à grande autonomie (les batteries performantes, elle connaît ça). Il a suffi de quelques chercheurs invités de l'université de Cambridge pendant trois semaines pour que les secrets du prototype s'envolent.


2 - Notre bonne surprise cette année fut de former des ingénieurs et des gestionnaires à voir venir et à anticiper les méthodes de manipulation hostiles lors de congrès, de salons d'exposition et de voyages ou simplement dans le quartier où se trouvent les bureaux.

- Je vous donne un truc : ce ne sont jamais les questions qui sont indiscretes, ce sont vos réponses.
- Il y a les questions logiques de la part d'un client potentiel inconnu et celles qui sont intrusives. Vous n'êtes jamais obligé d'y répondre.



**Autre article à lire sur le blog de l'auteur**

Cyber-Séductrices : Quand les Hironnelles hackent les secrets.

 **CLIQUER ICI**

Cyber-Séductrices : Quand les Hironnelles hackent les secrets. (sarx.net)

# Sécurité de l'information : le mirage de la cybersécurité et de la confidentialité

## Stop à la naïveté en sécurité de l'information!

Vous pensez qu'assurer la confidentialité de l'information en cybersécurité vous sauvera?

### Pure folie.

La cybersécurité et la confidentialité ne sont que la pointe de l'iceberg. Si vous négligez les autres piliers et caractéristiques de la sécurité de l'information, préparez-vous à un désastre.

C'est l'heure de la vérité brutale. Êtes-vous vraiment prêt?



par Francis Coats, ing. PSP CISSP

in

Expert en sécurité  
Sécurité physique, sécurité de l'information,  
cybersécurité et technologies

C'est parti pour la  
chasse aux licornes!





L'efficacité de la résilience en sécurité de l'information, particulièrement dans des situations de crise, est souvent mal évaluée en raison de l'erreur répandue de résumer cette sécurité à la protection de la confidentialité via la cybersécurité.

Les plans de continuité et de reprise après sinistre, bien que fondamentaux, ne sont pas suffisants sans une évaluation précise des risques spécifiques à chaque contexte.

Protéger des actifs informationnels sans une connaissance approfondie de leur existence ou des menaces potentielles est une démarche vouée à l'échec. Une préparation adéquate en matière de sécurité de l'information nécessite une identification et une compréhension approfondies des actifs ainsi que des menaces et vulnérabilités les concernant. Voyons deux erreurs à éviter.

### La confidentialité, garante de la sécurité de l'information

#### → PREMIÈRE ERREUR!

Il est crucial de remettre en question certaines idées répandues dans le domaine de la sécurité de l'information, notamment la perception erronée que la confidentialité est l'unique garant de la sécurité. En réalité, la sécurité de l'information englobe bien plus que la cybersécurité, s'appuyant sur la triade fondamentale :

- disponibilité (availability),
- intégrité (integrity)
- et confidentialité (confidentiality).

Cette triade est appelée **DIC** en français ou **CIA** en anglais. Ces trois caractéristiques sont essentielles et doivent être analysées et priorisées pour une sécurité effective.

#### De quoi est-il question?

La confidentialité vise à restreindre l'accès à l'information aux seules entités autorisées. L'intégrité assure l'exactitude et la complétude de l'information, tandis que la disponibilité garantit que les informations nécessaires sont accessibles aux utilisateurs autorisés au moment opportun.

Se concentrer exclusivement sur l'un de ces aspects au détriment des autres peut compromettre la sécurité globale de l'information si ce choix n'est pas fondé sur une décision éclairée et documentée, mais simplement sur la pire erreur de notre temps : considérer que ce qui est important, c'est la confidentialité de l'information garantie par la cybersécurité!

## Considérons trois scénarios dans une pharmacie illustrant l'importance de chaque caractéristique de la triade DIC :

- Le **premier scénario** montre une atteinte à la **confidentialité** avec la divulgation de dossiers personnels, un incident de sécurité souvent jugé inacceptable.
- Le **deuxième scénario**, qui concerne la **disponibilité**, implique un retard dans la délivrance d'une ordonnance causé par une mise à jour logicielle. Une situation frustrante, mais généralement moins critique à la pharmacie du coin.
- Le **troisième scénario**, qui touche **l'intégrité**, concerne la remise d'un mauvais médicament ou dosage, un manquement grave pouvant mettre en danger la vie. Ce dernier scénario l'emporte largement sur les deux premiers.

Ces exemples montrent l'erreur de prioriser une caractéristique de la triade DIC sans fondement ou questionnement, menant à des stratégies de sécurité inadaptées.

Par exemple, dans un contexte médical, la disponibilité de l'information peut s'avérer plus cruciale que sa confidentialité, comme le souligne l'exemple des bracelets MedicAlert.

Cette approche reconnaît l'importance de rendre certaines informations médicales facilement accessibles en cas d'urgence, valorisant la disponibilité par rapport à la confidentialité.

## La cybersécurité garantit la sécurité de l'information

### → DEUXIÈME ERREUR!

L'étymologie des termes « sécurité » et « information » nous offre une perspective enrichissante sur leur signification profonde. La sécurité de l'information ne se limite pas à la défense contre des intrusions numériques, mais implique une protection globale de l'intégrité, de la confidentialité et de la disponibilité des informations, nécessitant une variété de mesures de protection.

Historiquement, la sécurité de l'information a toujours été une préoccupation, dès l'apparition du langage il y a environ 100 000 ans. La disponibilité de l'information se manifestait par l'échange verbal de connaissances, l'intégrité était maintenue par des méthodes mnémotechniques comme les rimes et les légendes, et la confidentialité était contrôlée par des rites de passage limitant l'accès à des informations spécifiques.

Ces pratiques anciennes illustrent les fondements de la sécurité de l'information, mettant en évidence la nécessité d'un filtrage de sécurité, ou « habilitation de sécurité », comme premier pilier fondamental.

**“ Se concentrer exclusivement sur l'un de ces aspects au détriment des autres peut compromettre la sécurité globale de l'information. ”**

*Francis Coats ing. PSP CISSP*

Il y a près de 40 000 ans, avec l'évolution du langage symbolique et l'invention de l'écriture, de nouvelles dimensions de la sécurité de l'information ont émergé. La protection des informations écrites contre les intempéries, l'authentification des copies par des sceaux et l'utilisation du chiffrement ont été développées pour protéger les caractéristiques de la triade, mettant en évidence la nécessité de la sécurité physique comme deuxième pilier fondamental.

Finalement, il y a moins de 100 ans, l'avènement des technologies de l'information modernes a introduit un troisième pilier : la sécurité des technologies de l'information, ou « cybersécurité ». Cette ère a nécessité des approches spécifiques pour chaque caractéristique de la triade DIC, telles que des sauvegardes régulières pour la disponibilité, des empreintes cryptographiques pour l'intégrité et des méthodes de chiffrement avancées pour la confidentialité.

La sécurité de l'information est un domaine complexe qui nécessite une compréhension approfondie et une approche holistique, reconnaissant l'importance des caractéristiques de la triade DIC et des piliers de la sécurité de l'information.

Établir de manière éclairée la priorité entre confidentialité, intégrité et disponibilité selon le contexte est crucial pour élaborer des stratégies de sécurité efficaces.

De plus, il est essentiel de ne pas limiter la sécurité de l'information à la cybersécurité, mais de comprendre son essence, comme la protection globale des connaissances contre diverses menaces en intégrant le filtrage de sécurité, la sécurité physique et, finalement, les technologies de l'information pour une résilience maximale correspondant à la situation.

**Francis Coats, ing. PSP CISSP**

Qualifié par certains médias québécois comme l'un des experts en sécurité les plus reconnus, il démantèle les mythes de la sécurité. Enseignant à HEC, à l'ÉTS et au Hackfest, sa devise est : « La meilleure manière de contourner quelque chose qui ne se contourne pas, c'est de le contourner! »

<https://www.perf.etsmtl.ca/>



Pour regarder la vidéo cliquer sur l'image

# Développer une approche holistique de la sécurité de l'information

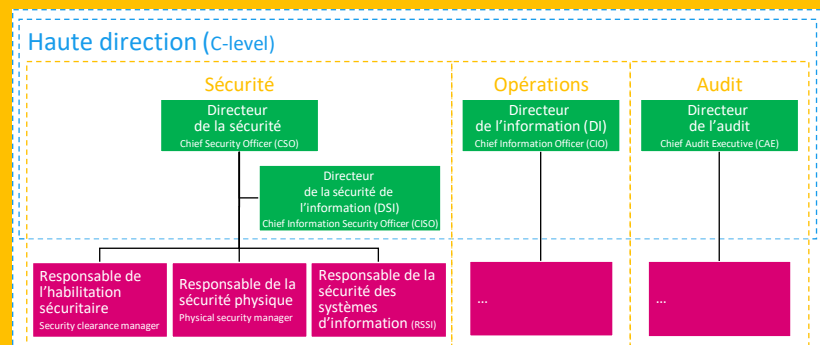
## Application pratique de la triade DIC

1. Inventorier tous les actifs, tangibles et intangibles, depuis les serveurs jusqu'aux bases de données.
2. Créer un tableau de référence pour évaluer uniformément la confidentialité, l'intégrité et la disponibilité des actifs.
3. Attribuer trois cotes de sécurité (DIC) en se basant sur ce tableau pour représenter la valeur de chacun des actifs.
4. Intégrer ces cotes dans l'évaluation des menaces et des risques pour hiérarchiser la protection des actifs et déterminer les mesures de protection appropriées.
5. Réévaluer périodiquement ces cotes pour rester à jour avec les changements dans l'environnement.

## Application pratique des piliers en sécurité de l'information

1. Vérifier les compétences du responsable : s'assurer que le directeur de la sécurité de l'information (DSI) possède des connaissances approfondies en filtrage de sécurité, en sécurité physique et en cybersécurité.
2. Structurer les départements : organiser les départements de cybersécurité, de filtrage, de sécurité en ressources humaines et de sécurité physique pour qu'ils relèvent directement et conjointement du directeur de la sécurité et du DSI.
3. Établir une hiérarchie claire : placer ce responsable sous l'autorité directe du directeur de la sécurité (CSO [chief security officer]), la plus haute instance décisionnelle de l'organisation en matière de sécurité.
4. Intégrer les piliers dans les évaluations : inclure les trois piliers de la sécurité de l'information dans chaque évaluation des menaces et des risques, assurant une couverture complète des aspects de sécurité.
5. Ne pas mélanger les rôles relatifs à la sécurité, aux opérations et à l'audit.

## Exemple de structure organisationnelle



Vendredi 17 h 48

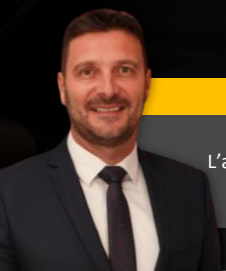
mon ordinateur ne fonctionne plus et toi ...

Vous êtes-vous déjà réveillé en sursaut en pleine nuit parce que vous aviez été cyberattaqué?

Non?

C'est parce que ça ne vous est pas encore arrivé.

Rassurez-vous, ça va arriver vite 😁.



par Frédéric Loisel



Président d'Armoring  
L'anticipation, l'organisation et la gestion du risque  
cyber constituent mon leitmotiv





🚨 **17 h 52**, je reçois l'alerte : une cyberattaque vient de démarrer au sein de mon entreprise. Un ordinateur est hors service, et mon téléphone portable commence à sonner.

📱 **17 h 58**, des SMS arrivent en cascade. Je sens déjà que la journée n'est pas terminée...

### État de la menace

Il ne se passe pas un jour sans que les médias spécialisés ne rapportent des cas d'entreprises, d'organisations ou d'administrations victimes de cyberattaques.

Pourtant, l'année 2024 s'annonce comme une période exceptionnelle pour l'Europe, et la France en particulier, pour plusieurs raisons.

Entre les conflits armés aux portes de l'Europe, les élections européennes prévues entre le 6 et le 9 juin 2024, l'organisation des Jeux olympiques du 26 juillet au 11 août 2024, suivie par les compétitions paralympiques du 28 août au 8 septembre 2024, et l'élection présidentielle américaine en novembre 2024, les enjeux sont considérables.

À cela s'ajoutent les nouveaux outils d'intelligence artificielle mis à la disposition du grand public, tels que les modèles de langage à grande échelle (LLM), qui permettent de générer rapidement de vastes quantités de texte, des images réalistes et, bientôt, des vidéos d'une qualité impressionnante.

Pour la première fois, nous disposons d'outils pouvant être facilement automatisés afin d'inonder les réseaux sociaux de données, avec la volonté de déstabiliser un pays, une économie et, par conséquent, les entreprises.

### Les entreprises face à la cybersécurité

L'annonce récente par l'État français de restrictions budgétaires de l'ordre de 10 milliards d'euros pour l'année 2024 nous démontre que le contexte économique est loin d'être prospère.

Les grandes entreprises internationales et nationales, ayant déjà affronté menaces et cyberattaques pendant de nombreuses années, ont intégré la culture de la cybersûreté au cœur de leurs systèmes de défense, et elles y allouent des budgets conséquents.

En revanche, un grand nombre d'ETI (entreprises de taille intermédiaire) et de PME ne disposent pas encore d'un niveau de sécurité et de sûreté adéquat pour continuer ou reprendre leurs activités à la suite d'une attaque ou d'incident informatique.

Toutefois, une prise de conscience est en marche depuis quelque temps parmi les dirigeants d'entreprise, stimulée par les retours d'expérience réalisés lors de conférences ou au sein de leur réseau professionnel.

### Problèmes rencontrés

D'après mes observations et les échanges que j'ai pu avoir avec des confrères, il apparaît clairement que l'installation d'un EDR (endpoint detection and response) et d'un pare-feu et la mise en place de sauvegardes ne constituent pas en soi une stratégie de cybersûreté complète, surtout lorsqu'aucun test d'intrusion et de restauration de sauvegarde n'a été réalisé.

**“Il ne se passe pas un jour sans que les médias spécialisés ne rapportent des cas d’entreprises, d’organisations ou d’administrations victimes de cyberattaques.”**

*Frédéric Loisel*

Bien que ces mesures ne soient pas inutiles, elles sont souvent perçues comme des solutions adoptées à un moment donné pour un besoin spécifique, sans nécessairement s’inscrire dans une vision globale de la gestion des risques et de la protection des actifs essentiels de l’entreprise.

La France s’attend à plus de 4 milliards de cyberattaques sur son territoire durant les Jeux olympiques. Il apparaît évident que les entreprises qui n’y sont pas préparées risquent inévitablement de subir des conséquences et des dommages.

Les entreprises prennent progressivement conscience de la nécessité de protéger leur système d’information, tout comme elles le font en verrouillant portes et fenêtres avant de quitter leurs bureaux.

Cependant, cette vigilance ne doit pas se limiter à la prévention. Il est crucial d’anticiper la possibilité d’une intrusion réussie par un cyberattaquant et de mettre en place des stratégies de gestion de crise efficaces pour y faire face.

### **Absence de solution universelle**

Il n’existe malheureusement pas de solution miracle applicable à toutes les entreprises.


Chaque organisation étant unique, les stratégies de cybersécurité doivent être personnalisées. Néanmoins, il est possible d’adopter certaines bonnes pratiques universelles.

Sensibilisez votre personnel : les erreurs humaines constituent fréquemment le point d’entrée favori des cyberattaquants dans vos systèmes d’information.


En parallèle, réalisez une analyse des risques afin de déterminer les actifs les plus critiques à protéger, ce qui devrait mener à l’élaboration d’un plan de continuité d’activité (PCA).

Il est également essentiel d’organiser des exercices de gestion de crise, en privilégiant les scénarios les plus probables liés à votre secteur d’activité.



 Il est impératif de ne pas remettre ces exercices à plus tard, sous prétexte que votre système n'est pas entièrement sécurisé; les cybercriminels, eux, n'attendent pas.

La préparation et la répétition des procédures d'urgence sont capitales pour mesurer l'ampleur des potentiels incidents et pour savoir comment réagir efficacement. « L'entraînement permet de mieux gérer les situations de crise réelles. »

 **18 h 20**, le centre de sécurité supervisant mon système d'information m'informe que la situation est maîtrisée.

Le poste de travail de l'employé ayant ouvert une pièce jointe malveillante a été isolé. Pour l'instant, aucun indice ne justifie le déclenchement d'une gestion de crise, mais nous maintenons une vigilance accrue pour les prochaines 48 heures.

**La sécurité et la sûreté, tant matérielles qu'immatérielles, sont l'affaire de tous.**

**Frédéric Loisel**



Ancien Officier marinier de la Marine nationale française dont quatre années en Centre de Secours et Sauvetage en Mer

Plus de 20 ans d'expérience en tant que responsable informatique dans différentes PME.

Co-fondateur de la société Armoring en mars 2024.

<https://www.armoring.fr/>

## Mes quatre points clés pour la sécurité des systèmes d'information

- 1. Anticipez :** réalisez un audit des risques sur votre système d'information pour identifier ce qu'il est crucial de protéger, et sensibilisez régulièrement vos salariés. C'est toujours plus facile de travailler hors crise.
- 2. Préparez :** installez un système de détection et d'alerte. Préparez-vous à divers scénarios d'attaque et validez vos procédures grâce à des exercices afin de développer les bons réflexes pour une réaction efficace.
- 3. Protégez :** sécurisez vos informations vitales et établissez un plan de continuité d'activité (PCA) ou un plan de reprise d'activité (PRA) pour ne pas être vulnérable en cas d'incident ou d'attaque.
- 4. Améliorez :** insistez sur l'amélioration continue. Votre système d'information évolue, tout comme les méthodes d'attaque. Maintenez une veille constante et testez régulièrement vos procédures.

D'autres aventures à suivre... 



## Aller plus loin avec les formations et ateliers de Crise & Résilience

Formation & Simulation

**Initiation à la gestion de Cyber Crise & vivre une simulation de crise**

1 journée

[En savoir +](#)

Atelier & Formation

**Mettre en place votre plan de gestion de Cyber Crise**

5 demi-journées

[En savoir +](#)

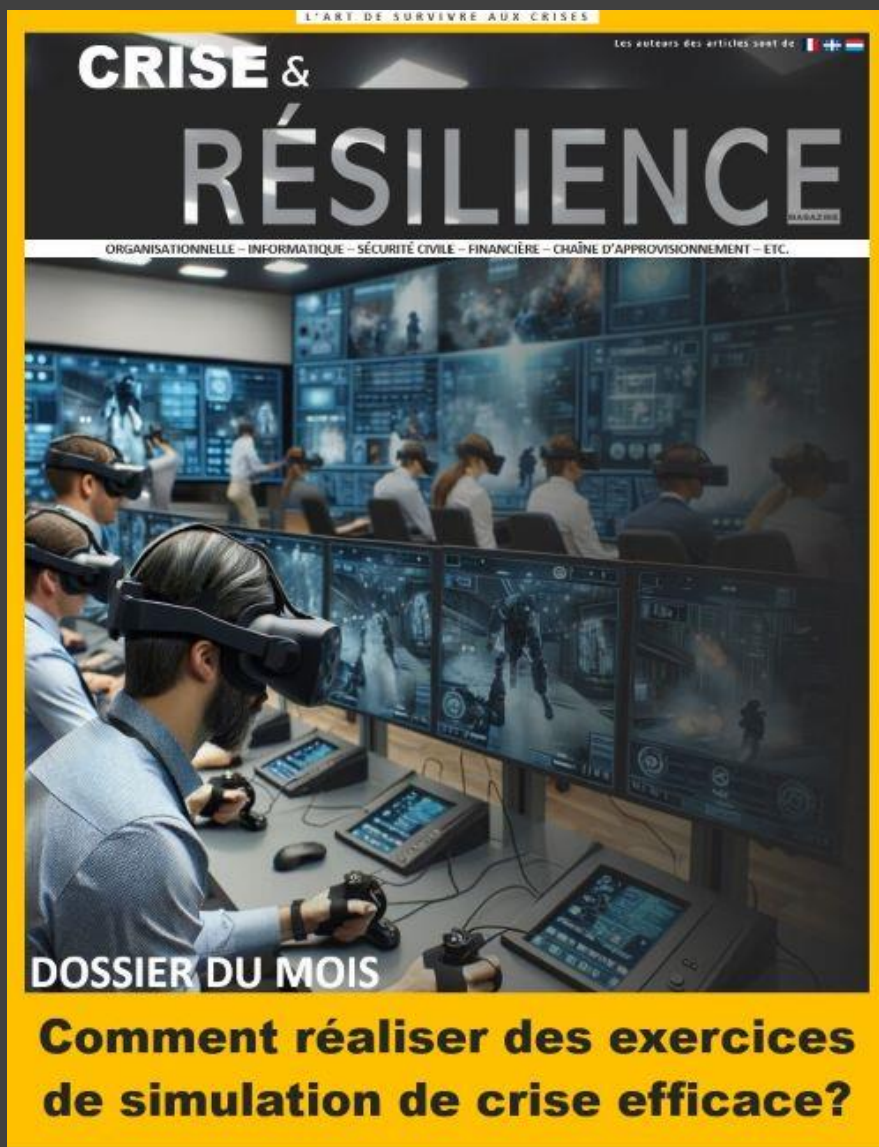
Atelier pratique & Simulation

**Mettre en place des exercices et construisez votre prochaine simulation de Cyber Crise**

1 journée

[En savoir +](#)

# RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

[www.CriseEtResilience-Magazine.com](http://www.CriseEtResilience-Magazine.com)

CRISE &

# RÉSILIENCE

C'EST...  
AUSSI

Une chaîne  YouTube avec...

Des conférences et formations gratuites



Des interviews d'experts :

 <p><b>D'EXPERTS</b> Déjouer les risques. 5 idées vraies pistes pour les c... 1:21:23</p>	 <p><b>D'EXPERTS</b> Comment apporter les techniques du survivalisme à l'en... 34:49</p>	 <p><b>D'EXPERTS</b> Le rôle du Responsable de Continuité d'Activité... 42:15</p>	 <p><b>PAROLE D'EXPERTS</b> Cyberattaque Quelles sont les erreurs à ne pas... 14:49</p>	 <p><b>PAROLE D'EXPERTS</b> NÉGOTIATION négocier avec les cyber... 46:17</p>
Comment déjouer les risques : - 5 idées reçues - Interview...	Comment apporter les techniques du survivalisme ...	Gestion de Crise & Continuité des Activités: Expertise de...	Cyberattaque : Les erreurs à ne pas faire - Parole d'exper...	Les conseils d'un expert pour faire face aux demandes de...

Des réponses à vos questions :

 <p><b>LA QUESTION DU LUNDI</b> C'est quoi la Cyber Résilience? Versus la Cyber sécurité... 2:39</p>	 <p><b>La question du Lundi</b> Pourquoi notre logo est une fourmi? 3:07</p>	 <p><b>LA QUESTION DU LUNDI</b> Assurance et/ou plan de continuité? 2:10</p>	 <p><b>LA QUESTION DU LUNDI</b> Est-ce trop tard pour un plan de continuité? 3:27</p>	 <p><b>LA QUESTION DU LUNDI</b> Êtes-vous un poisson? HAMEÇONNAGE PARTIE 1 Les pièges 2:42</p>
C'est quoi la Cyber Résilience et quelle différence avec...	Pourquoi notre Logo est une fourmi   Rapport avec la...	Plan de continuité d'activité et/ou assurance	Plan de continuité des affaires est-ce trop tard pou...	Hameçonnage et continuité des affaires - Quel sont les...

Une page  avec...

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



Dans cet article, je vous invite à explorer différentes approches de la cyberrésilience, basées sur son expérience acquise sur d'autres continents, en Amérique et dans le Pacifique. Découvrez comment certaines leçons apprises ailleurs peuvent être bénéfiques ici!



par **Dimitri Souleliac**



Directeur, consultation en cybersécurité  
Gouvernance, audit et gestion des risques  
en matière de cybersécurité

**“La résilience des processus d'affaires consiste à redémarrer les opérations de production rapidement en mode dégradé, pendant que les équipes informatiques rétablissent les systèmes et effectuent les vérifications nécessaires.”**

*Dimitri Souleliac*

La cyberrésilience est une priorité pour les entreprises, qui sont confrontées à une augmentation des risques naturels et des risques en matière de cybersécurité.

Cependant, la perception du danger et les stratégies de préparation diffèrent selon les régions, façonnées par des contextes culturels et environnementaux. C'est avec enthousiasme que je vous fais part de mon expérience, naviguant entre Amérique et Pacifique.

### **Perception du risque de catastrophe**

Au Québec, il existe un sentiment de sécurité et de protection à l'égard des cyberattaques. Beaucoup de gestionnaires croient que la province est moins susceptible d'être touchée par des catastrophes informatiques.

C'est une perception souvent alimentée par une sous-estimation du risque. Cette attitude peut s'avérer dangereuse, car elle peut mener à un manque de préparation face à des attaques potentiellement dévastatrices.

Le Québec n'est pas situé en zone de conflit; toutefois, les cyberattaques ne connaissent pas de frontières, ni géographiques ni linguistiques.

### **La cyberrésilience vue d'ailleurs**

De mon expérience récente dans le Pacifique, notamment en Nouvelle-Zélande, j'ai observé une plus grande préoccupation pour les risques naturels (séismes, inondations et tsunamis), en raison du contexte géologique et insulaire.

Cette conscience du risque engendre une culture de préparation et d'adaptation, qui se reflète dans le domaine de l'informatique.

Un exemple intéressant de collaboration et de préparation est celui de la communauté de Christchurch sur l'île du Sud, qui, à la suite des séismes de 2010 et de 2011, a développé une infrastructure robuste incluant désormais la résilience.

Concrètement, la résistance est le fait de ne pas s'effondrer en cas de séisme, alors que la résilience est la capacité des personnes à retourner utiliser les infrastructures le plus rapidement possible, après que les ingénieurs ont effectué les vérifications nécessaires.

Cet exemple s'applique très bien aux incidents informatiques.

La résilience des processus d'affaires consiste à redémarrer les opérations de production rapidement en mode dégradé, pendant que les équipes informatiques rétablissent les systèmes et effectuent les vérifications nécessaires. Notamment, en cas de cyberattaque, l'adversaire peut persister dans l'environnement.

Il est donc impératif de contenir et d'éradiquer la menace avant de restaurer les systèmes, ce qui n'est pas vraiment le cas lors d'un désastre naturel.

### **Se préparer et s'entraider**

Dans le Pacifique, j'ai échangé avec des entreprises qui ont développé des stratégies uniques pour assurer la continuité de leurs opérations.

Par exemple, elles utilisent des serveurs montés sur des systèmes antisismiques ou ont mis en place des accords avec des exploitations agricoles pour la fourniture de diesel en cas de coupures de courant prolongées.



J'ai rencontré des gestionnaires qui, face aux risques, ont une compréhension profonde de leurs opérations critiques. Ils privilégient des solutions simples et une collaboration étroite avec leurs clients et partenaires pour fonctionner en mode dégradé.

Lors d'une cyberattaque, j'ai vu des personnes de secteurs d'affaires se porter volontaires pour réinstaller des ordinateurs à l'aide de clés USB et d'une procédure simple. Ce sont aussi des PME qui ont le réflexe d'appeler leur compétiteur pour obtenir de l'assistance.

À l'aide de systèmes de plan de continuité et de relève informatiques conjoints ou réciproques, les entreprises peuvent faire face ensemble à des risques qui sont hors de leur contrôle. Ce fut le cas lors du cyclone Gabrielle, qui a affecté l'île du Nord et la région d'Auckland en février 2023.

Ce sont parfois des solutions évidentes, comme le déploiement de liens de secours Internet par satellite grand public, qui a été un facteur clé de succès. Dans l'urgence, j'ai vu des professionnels en cybersécurité apporter leur assistance pour garantir un bon niveau de confidentialité et d'intégrité lors des interventions visant à rétablir la disponibilité des systèmes et des moyens de communication.

Le déploiement d'ordinateurs, de médias amovibles ou de liaisons Internet de secours ne doit pas négliger les processus de sécurité (correctifs de sécurité, endurcissement, chiffrement, etc.). Ce principe est d'ailleurs très bien décrit dans la clause 5.29 de la norme ISO 27002:2022, qui exige le maintien de la sécurité de l'information lors de la continuité et de la relève.

### Partager les leçons apprises

Ces cas concrets sont des enseignements précieux pour les autres régions du monde, où une augmentation de la résilience et de la préparation pourrait grandement bénéficier aux organisations.

Adopter une approche proactive, axée sur la compréhension des opérations essentielles et des vulnérabilités et sur le développement de partenariats solides, pourrait améliorer la capacité des entreprises à résister, mais surtout à se rétablir face aux cyberattaques et aux désastres naturels.

Les entreprises de taille moyenne (environ 50 employés pour la Nouvelle-Zélande et 100 pour le Québec) peuvent compter sur un plus grand niveau d'agilité. De plus, certaines façons de faire, apprises dans les plus petites structures, peuvent s'appliquer facilement, surtout en contexte d'urgence, où il est essentiel d'aller... à l'essentiel!

La cyberrésilience ne se limite pas à la mise en place de technologies avancées. Elle exige également une compréhension claire des risques spécifiques à chaque environnement et une préparation adaptée.

Les exemples que j'ai donnés de mon expérience dans le Pacifique démontrent l'importance d'une approche pragmatique, intégrant la préparation aux désastres naturels et aux risques en matière de cybersécurité et basée sur la collaboration.

Les entreprises auraient tout à gagner à s'inspirer de ces modèles pour développer leur propre résilience face à un paysage de menaces en constante évolution.

### Dimitri Souleliac

Dimitri Souleliac est directeur chez Coresilium, une firme dédiée à rendre la cybersécurité simple, accessible et applicable. Certifié CISSP, CISM et ISO 27001 Lead Implementor, Dimitri propose des services de consultation en cybersécurité indépendants et orientés sur les objectifs d'affaires.



<https://www.coresilium.com/>







## 3 conseils pour augmenter votre cyberrésilience

- **Ayez une trousse d'urgence avec des solutions simples** : votre kit (trousse) de survie informatique devrait contenir l'essentiel pour reconstruire votre système informatique à partir de zéro (documentation papier, clés USB, ordinateurs portables de secours, logiciels de base, clés d'authentification forte, clés de chiffrement, téléphones avec accès Internet 4G/5G ou satellite).
- **Collaborez et entraidez-vous** : la collaboration entre entreprises montre l'importance de la solidarité en cas de crise. Réfléchissez à un partenariat d'assistance et d'échange de ressources, à l'utilisation de plans de continuité et de relève informatique conjoints ou réciproques, et même, dans certains cas précis, au volontariat interne pour rétablir vos systèmes. Ce sont des pratiques qui renforcent la résilience des entreprises et de la communauté.
- **Adoptez une culture axée sur la préparation et l'adaptation** : inspirée par les stratégies de réponse aux catastrophes naturelles, cette culture vous permet de vous préparer à faire face à un incident et à vous rétablir rapidement à la suite de ce dernier. En cas de cyberattaque, apprenez à vous adapter à la situation, car les scénarios sont bien plus incertains qu'un cas de feu ou d'inondation. L'objectif est d'accélérer la relève de vos opérations les plus critiques.

Visionnez des dizaines d'interview sur la chaîne YouTube de **Cyber Crise**



# Données possiblement « perdues » Voici la solution de la dernière chance!

Plongez dans le monde de la récupération des données après une cyberattaque, où chaque bit perdu est une pièce du puzzle à reconstituer.

Découvrez les techniques innovantes et les stratégies de récupération qui défient l'obscurité numérique pour ramener vos données précieuses à la lumière.

Explorez l'art de la résilience numérique et laissez-vous surprendre par la magie de la restauration des données perdues.



par **Christophe Vanypre**



Directeur

Gestionnaire de la cellule de réponse d'urgence,  
gestion de crise et remédiation



**“41 % de ceux qui ont payé une rançon aux cybercriminels n’ont pas réussi à récupérer toutes leurs données!”**

*Rapport Hiscox 2022*



La récupération de données en laboratoire est une option trop souvent oubliée ou méconnue postcyberattaque. Or, il s’agit de la seule solution de rechange au paiement de la rançon lorsque les données sont altérées, d’autant que payer la rançon n’est pas l’assurance tous risques qui permet de récupérer toutes les données avec certitudes.

Selon le rapport Hiscox 2022, 41 % de ceux qui ont payé une rançon aux cybercriminels n’ont pas réussi à récupérer toutes leurs données.

Si l’intérêt d’un plan de reprise des activités (PRA) n’est plus à prouver, on vous démontre pourquoi il est indispensable d’inclure cette étape dans votre PRA.

## **L’intégration de la récupération de données dans un PRA, une étape cruciale, voire indispensable dans la remédiation postcyberattaque**

Dans le paysage numérique actuel, les entreprises sont confrontées à une menace constante de cyberattaques.

Les ransomwares, en particulier, ont le pouvoir de paralyser complètement une organisation en chiffrant une partie de ses données afin de les rendre toutes inaccessibles, et en exigeant une rançon. C’est pourquoi il est essentiel de prendre des mesures proactives pour faciliter la remédiation en cas d’attaque.

L’une de ces mesures cruciales consiste à créer un PRA et à y inclure la récupération de données via un laboratoire.

### **Comprendre l’importance du PRA**

Un PRA est une stratégie de gestion de crise qui permet à une entreprise de continuer à fonctionner en cas de catastrophe ou d’incident majeur. Il inclut généralement des procédures détaillées pour restaurer les systèmes informatiques et les données critiques.

L’objectif est d’appliquer rigoureusement les étapes imaginées en de pareilles circonstances.

Cependant, de nombreuses organisations négligent l’importance de la récupération de données dans leur PRA, pensant que les mesures de sécurité mises en place et les sauvegardes suffisent à les sécuriser.

### **Le rôle de la récupération de données postcyberattaque**

Lorsque l’ensemble des données présentes sur les backups sont altérées, c’est là qu’intervient la récupération de données.

En intégrant cette étape dans votre PRA, vous vous assurez que votre entreprise dispose d’un plan clair pour restaurer rapidement l’accès à vos données cruciales en cas de cyberattaque.

Par ailleurs, l’intégrer dans votre plan permet d’éviter toutes actions hâtives qui entraveraient ensuite la récupération de données.

Nous constatons trop souvent des organisations qui ont voulu repartir très vite en formatant des serveurs, avant de s’apercevoir que la seule solution est de faire appel à nous pour accéder aux données.

Pour éviter cela, nous pouvons également proposer un clonage bit à bit avec blocage en écriture, ce qui permet de figer la situation sans altérer les supports ni même les éventuelles opérations de forensique.

## Les avantages d'une récupération de données

La mise en place d'un processus robuste de récupération de données offre de multiples bénéfices cruciaux aux organisations, notamment :

- 1. Minimisation de la durée d'indisponibilité** : en ayant un processus de récupération de données bien défini, vous pouvez réduire le temps d'indisponibilité de vos systèmes, minimisant ainsi l'impact financier et opérationnel.
- 2. Réduction des coûts** : plutôt que de payer une rançon aux cybercriminels, vous pouvez récupérer vos données en laboratoire afin de les restaurer au jour de l'attaque, pour un coût très largement inférieur au montant de la rançon. Et ce, contrairement à la restauration d'un ancien backup, qui implique de nombreux jours de travail perdus à rattraper.
- 3. Réputation** : une réponse rapide et efficace à une cyberattaque renforce la confiance de vos clients et partenaires, préservant ainsi la réputation de votre entreprise.
- 4. Seule solution de rechange au paiement de la rançon** : lorsque l'ensemble des données sont altérées, y compris sur les backups, la récupération de données est la seule solution de rechange au paiement de la rançon.

N'oublions pas que payer la rançon revient à devenir un bon client pour les hackers. Il n'est en effet pas rare de voir une entreprise rapidement réattaquée après avoir payé une rançon.

**Selon le rapport Hiscox 2022, plus du tiers (36 %) des entreprises qui ont payé une rançon à des cybercriminels ont été ciblées une deuxième fois.**

- 5. En cas de vol de données** : lorsque les données ont été capturées par les hackers qui menacent de les diffuser, les actions de récupération de données permettent de réduire la valeur objective de la rançon.

Dans ce cas, si la cible attaquée souhaite payer la rançon, elle le fera uniquement pour éviter la diffusion des données sans demander la clé de décryptage, ce qui facilite la négociation forte du montant de la rançon. Les économies réalisées sont bien supérieures au coût d'une récupération de données.

En conclusion, nous constatons bien trop souvent, au sein de nos laboratoires, que la récupération de données est une réflexion après coup lorsqu'une cyberattaque se produit. Or, elle devrait être une composante intégrale de votre plan de reprise d'activité pour enrayer les cyberattaques.

En investissant dans une planification proactive, vous pouvez renforcer la résilience de votre entreprise face aux menaces numériques croissantes.

### Christophe Vanypre

Recoveo, numéro un français de la récupération de données, est présent à Paris (08) et au nord de Lyon. Chaque semaine, nous facilitons la remédiation de sociétés ou d'organisations victimes d'une cyberattaque, sans avoir à payer la rançon aux hackers. Le tout en garantissant la souveraineté de vos données.

Depuis 2017, notre cellule de recherche et développement est active afin de nous permettre de récupérer les données post-ransomware sur tout type d'environnement au sein de nos laboratoires.

Nous travaillons très souvent en collaboration avec de nombreux experts en cybersécurité afin d'optimiser les délais en coordonnant les actions et les priorités.



<https://www.recoveo.com/>





## Les critères pour bien choisir son prestataire de récupération de données

Choisir le bon prestataire de récupération de données après une attaque par ransomware est crucial pour la restauration efficace de vos informations. Pour cela, quatre critères sont primordiaux :

1. **Expérience dans le domaine du ransomware** : il est impératif de vous assurer que le prestataire de récupération de données possède une solide réputation et une expertise avérée dans le domaine de la cybersécurité. Recherchez des retours d'expérience ou des pages Web permettant d'attester de leur capacité à gérer des incidents complexes de ransomware.

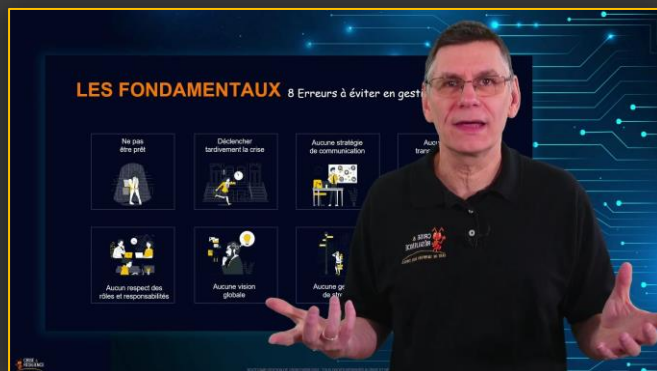
Assurez-vous également que le prestataire retenu maîtrise les technologies de votre environnement informatique, vos systèmes de backup et vos besoins spécifiques.

2. **La transparence** : un prestataire fiable doit être en mesure de vous fournir un aperçu clair de son processus de récupération de données. Assurez-vous de recevoir la liste des éléments récupérés en miniature, afin de pouvoir les visualiser avant de valider l'étape finale de récupération de données. Vous paierez ainsi la prestation en connaissance de cause. Cette liste vous permettra également d'orienter la récupération au fil de l'eau en fonction de vos priorités. Sans cela, difficile d'orienter votre prestataire vers vos priorités.
3. **La souveraineté de vos données** : les données que vous pouvez être amené à confier peuvent contenir des informations sensibles. En choisissant une société de récupération de données indépendante qui garantit la souveraineté des données, vous vous assurez que ces informations resteront confidentielles et ne seront pas exposées à des tiers non autorisés.
4. **Cellule d'urgence** : vous devez vous assurer que la société de récupération est joignable à tout moment et qu'elle est en mesure de mobiliser des équipes qui vous seront dédiées en tout temps.

En résumé, le choix d'un prestataire de récupération de données nécessite une évaluation minutieuse de son expertise afin que celui-ci devienne un partenaire efficace.

## 8 ERREURS À ÉVITER EN CAS DE CRISE

Extrait de la formation « Mettre en place une gestion Cyber Crise »



Pour regarder la vidéo, Cliquez sur l'image

# 5 conseils anti-stress simples et sans contraintes.

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



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

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



**Timothy Mirthil-de Segonzac**

Journaliste et auteur spécialiste de la gestion du stress



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

## La respiration Matrix

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

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

## Le magnésium magique

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

## La force de la marche

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

## Le sommeil, ton allié

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

## La confiance en toi

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

## Celui-ci... c'est cadeau 🎁

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

Voilà 5 conseils sans contraintes jeune homme.

# Passé à l'action!

# 4 techniques pour rester performant en période de crise

En cellule de crise, gérer son effort et sa récupération est le meilleur moyen d'être performant. Voici quelques techniques opérationnelles.

## Gestion du stress :

En cas de stress intense, utilisez la respiration triangulaire qui accentue l'expiration afin d'activer le nerf vague et clarifier vos idées.

Suivez le schéma 4-8-4 : inspirez profondément pendant 4 secondes, expirez pendant 8 secondes, puis retenez l'air pendant 4 secondes. Faites des cycles de 2 minutes dès que nécessaire.



## Gestion de la fatigue :

En cellule de crise, la fatigue est un ennemi silencieux.

Pour la surmonter dans l'urgence, équilibrez avec des pauses. Prenez régulièrement 5 minutes par heure pour bouger, vous hydrater et vous détendre mentalement. Le mouvement du corps repose l'esprit.



## Micro-sieste :

En cas de veille prolongée pendant une crise. Songez que le manque de sommeil équivaut à l'alcoolémie : 17 heures sans sommeil = 0,05g (21h = 0,08g et 24h = 0,10g).

Optez pour des "siestes flash" de 5 ou 10 minutes toutes les deux heures en vous concentrant sur votre respiration. Ou alors, si vous avez suffisamment d'opérateurs, alternez 1h d'activité avec 1h de sieste comme le font les pilotes long-courriers.



## Coordination :

Pour revitaliser l'équipe après une période difficile, pratiquez une respiration collective.

En cercle, bras sur les épaules des collaborateurs, inspirez profondément par le nez et expirez ensemble par la bouche, comme un soupir. Répétez trois fois. C'est une technique utilisée par le XV de France pour se remobiliser environ 5 ou 6 fois par match.



# Roumanie, à quoi bon un PCA sans test?

Au début de la pandémie de COVID-19, je me rappelle le nombre de sociétés roumaines qui m'ont contacté pour avoir des conseils en gestion de crise et de mise en œuvre pour faire face à la crise sanitaire, sollicitant en urgence un dossier de plan de continuité des activités (PCA) clés en main!



par Jean François Jund



Gérant de la société JFcontact SRL – Auditeur ISO 27001 et 22301

La veille sectorielle en sécurité et la gestion des risques en entreprise – auditeur et coach en sécurité et sûreté





En Roumanie, le PCA n'est pas obligatoire, sauf pour des entreprises aux activités particulières qui présentent un risque externe ou particulier.

Lors d'un sondage au début de la crise sanitaire, seuls environ 30 % des entreprises roumaines déclaraient disposer de documents de gestion de crise.

Le PCA, en Roumanie, était un domaine inconnu pour beaucoup d'entreprises avant la COVID. La pandémie et la mise en œuvre de mesures sanitaires ont donné du fil à retordre aux dirigeants et aux responsables de sécurité et de sûreté!

Mais, cela dit, après la pandémie, ça n'a pas déclenché un électrochoc supplémentaire pour faire des démarches de prévention et de préparation à la résilience.

Les risques existent et sont bien identifiés.

Par exemple, la Roumanie est le pays de l'Union européenne (UE) le plus exposé à un tremblement de terre majeur, une sorte d'épée de Damoclès, qui pourrait se déclencher à n'importe quel moment!

Les entreprises préfèrent négliger les aspects de sécurité qui souvent demandent des engagements financiers (audits, achats de matériel, formations) et qui peuvent prêter au questionnement au sein de l'entreprise.

Alors on préfère ne rien dire et ne rien faire, et miser sur la fatalité!

Lors de ce sondage, seuls 30 % des entreprises ont déclaré avoir des solutions pour intervenir lors d'une crise!

Parmi les entreprises qui disposent d'un PCA, on compte des multinationales ou des opérateurs locaux qui doivent respecter des mesures de sécurité en raison de la législation de leur secteur d'activité, comme les OIV (opérateurs d'importance vitale) – eau, gaz, électricité, télécommunications et énergie –, mais aussi le secteur bancaire, la chimie, la pétrochimie, la santé et les infrastructures de transport (terre, air, mer, chemin de fer, etc.).

Mais combien dans les 30 % ont des PCA qui ont été testés?

Difficile à dire... Lors des audits, on découvre souvent des dossiers de gestion de crise qui ne sont pas mis à jour ou des PCA qui traitent superficiellement du sujet.

Il est sans rappeler qu'un PCA n'a aucune valeur s'il n'a pas été testé ou déclenché au sein de l'organisation! Des exercices de simulation de crise en salle de type « table top » sont précieux pour valider et améliorer le PCA.

Au-delà de la documentation du PCA, qui, pour beaucoup, n'est qu'un dossier papier dans une bibliothèque, on constate l'absence d'une maturité dans les moyens techniques de mise en œuvre. En clair, pas de salle de crise dédiée avec des moyens adaptés pour gérer une crise et se préparer à la résilience.

Dans le cas de la Roumanie et du risque sismique pour les OIV, il est nécessaire d'avoir des locaux où l'on peut rester longtemps – salle de crise, salle de repos, cuisinette avec réserve d'alimentation (nourriture et eau) – et des moyens techniques comme un téléphone satellite, un récepteur Internet via satellite de type Starlink, des ordinateurs portables ou des tablettes disposant de la documentation technique disponible hors ligne...

Le sac de survie, en milieu urbain, peut être utile lorsqu'on doit rester autonome sur un site après le déclenchement d'une crise sévère. C'est un élément que l'on doit préparer impérativement en amont, en prévention d'une éventuelle crise, pour éviter de subir des contraintes supplémentaires.

Un autre risque important qui plane sur les entreprises roumaines est le risque cyber et une éventuelle attaque informatique.

Le point positif sur la gestion de crise cyber sera l'élaboration obligatoire d'un PCA en raison de l'arrivée prochaine de la mise en œuvre de la directive européenne NIS 2 (Network and Information Security).

La directive NIS 2, adoptée en décembre 2022, est un tournant majeur pour la cybersécurité en Europe. Elle vise à harmoniser les pratiques de cybersécurité dans l'UE et à élargir son champ d'application à un plus grand nombre d'entités, couvrant ainsi plusieurs secteurs d'activité.

De nombreuses entreprises seront concernées par la directive et devront obligatoirement mettre en œuvre un certain nombre de mesures de sécurité au sein de leur organisation.

**On note que la Roumanie a fait récemment l'objet d'importantes attaques cyber qui ont touché le Parlement roumain et un certain nombre d'établissements publics de santé. Les récents incidents montrent bien qu'on n'est absolument pas à l'abri d'une attaque. Et qu'une entreprise mal préparée, peu importe sa taille, aura beaucoup de mal à gérer la crise!**

Depuis plusieurs mois, la Roumanie, via son centre national de sécurité cybernétique (DNCS), fait de la sensibilisation au sujet du risque cyber en apportant aux entreprises les informations sur les attaques et les mesures de précautions à prendre.

Le constat est que, sans une législation du PCA, le dirigeant d'une société reste le maillon décideur dans l'entreprise. Une gestion de crise en entreprise n'arrive pas qu'aux autres.

**L'entreprise doit se préparer à la gestion de crise et à la résilience et doit accepter les investissements en prévention et en sécurité sur les plans humain et matériel. Afin de garantir sa survie!**

**Jean François Jund**

J'ai découvert la Roumanie en 1995 lors d'une mission en ex-Yougoslavie. J'ai été détaché de 2001 à 2004 dans le projet de restructuration de l'école des officiers de la gendarmerie roumaine. J'ai quitté l'armée en 2004 pour fonder ma propre entreprise, JFcontact SRL

[www.resiliency.ro](http://www.resiliency.ro) [www.frenchsecurityhub.ro](http://www.frenchsecurityhub.ro)

## **Bonus : La veille active reste l'outil de sécurité principal!**

Il n'y a pas de plan de sécurité sans une veille active sur les risques et l'évolution des risques dans l'environnement d'une entreprise. Un PCA doit rester impérativement à jour; il doit être vérifié et mis à jour annuellement ou à la suite d'un incident, d'un audit ou d'une simulation de crise. Au sein d'une organisation, il est important de garder une veille active sur les différents risques et menaces, mais aussi sur les moyens d'aide technologique disponibles.

À cet égard, il existe des revues spécialisées, et de nombreux salons dédiés à la sécurité sont organisés régulièrement avec des experts qui sont en mesure d'accompagner des entreprises et de mener des formations spécifiques (exercices de simulation de crise) pour les cadres dirigeants et le personnel. Il ne faut pas avoir peur d'externaliser un service, surtout quand il s'agit d'assurer la sécurité.

En exemple d'innovation technologique, durant les derniers mois sont apparues des applications pour smartphone qui permettent de mettre votre PCA sur votre téléphone et celui de vos collaborateurs impliqués dans la gestion de crise. Cela comporte plusieurs avantages : un suivi en direct du PCA lors de son déclenchement, la visualisation et la validation des différentes mesures par les acteurs de la cellule de crise, un enregistrement en direct et une sauvegarde du journal des événements!

# Ne laissez pas une crise paralyser votre entreprise !

## Voici comment assurer la continuité de vos activités en cas de crise

 Suivez cette formation pour



**Assurer la continuité des opérations** : de réagir rapidement et efficacement pour maintenir vos activités opérationnelles en toute situation.



**Réduire les risques** : d'identifier proactivement et de minimiser les risques potentiels, évitant ainsi des perturbations coûteuses.



**Améliorer la réputation de votre entreprise** : de démontrer un engagement envers la sécurité et la préparation, ce qui peut renforcer la confiance des clients et des partenaires.



**Gagner un avantage compétitif** : de vous positionner avantageusement face à la concurrence grâce à une meilleure préparation aux interruptions d'activité.

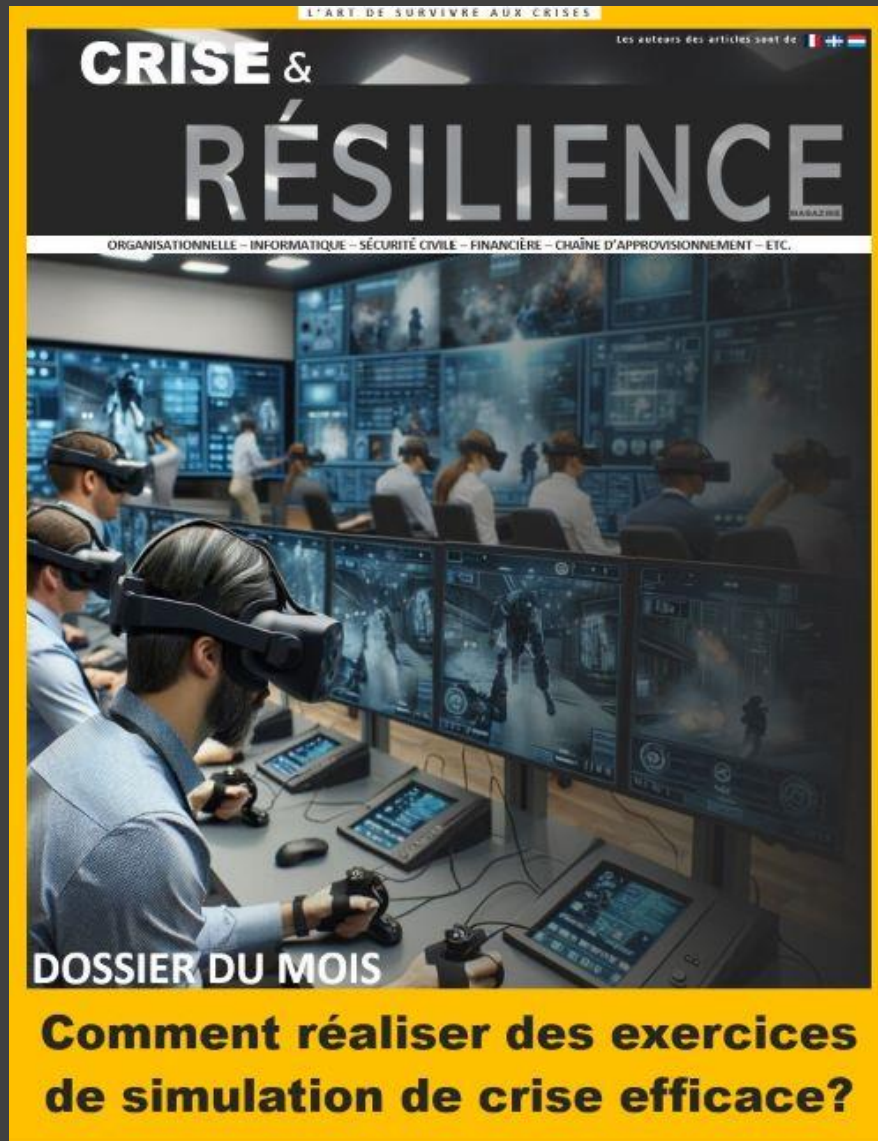


**Renforcer la résilience organisationnelle** : de contribuer à la création d'une culture d'entreprise axée sur la préparation et la gestion proactive des crises.



Cliquez ici, pour commencer à sécuriser votre futur.

# RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

[www.CriseEtResilience-Magazine.com](http://www.CriseEtResilience-Magazine.com)