L'ART DE SURVIVRE AUX CRISES

CRISE & RÉSILIENCE MAGAZINE

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

NUMÉRO 7 – JUILLET 2024

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

Responsable de la sécurité de l'information
ou… de la résilience de l'entreprise ?

Continuer l'enseignement
sans informatique

Technologie au service
de la résilience des entreprises

PRA spécial TPE/PME
Simple, efficace et accessible

Continuité d'activité
une démarche multidisciplinaire

Crise permanente
à marche forcée

DOSSIERS DU MOIS

Comment construire un exercice de gestion de crise

MAGAZINE OFFERT PAR CRISE & RÉSILIENCE

CRISE &

RÉSILIENCE C'EST... AUSSI

Une chaîne YouTube avec...

Des conférences et formations gratuites

Des interviews d'experts :

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 :

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 LinkedIn avec...

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

Édito

Chers lecteurs,

Bienvenue dans ce nouveau numéro de Crise & Résilience, votre magazine dédié à la gestion de crise et à la résilience des organisations.

Dans un monde en perpétuelle mutation, où les crises se succèdent et se complexifient, il est plus que jamais essentiel pour les entreprises de développer leur capacité à anticiper, à faire face et à rebondir. C'est tout l'enjeu de la résilience organisationnelle.

Au fil des pages de ce numéro, vous découvrirez des analyses pointues, des retours d'expérience inspirants et des conseils pratiques pour renforcer la résilience de votre organisation. Nos experts vous livrent les clés pour construire des exercices de gestion de crise efficaces, mettre en place un plan de reprise d'activité robuste ou encore assurer la continuité pédagogique en cas de cyberattaque.

Vous plongerez également dans les coulisses de la récupération de données, une expertise cruciale mais méconnue, à travers une interview passionnante. Et vous explorerez comment la technologie peut être mise au service de la résilience des entreprises.

Plus que jamais, la résilience doit être placée au cœur de la stratégie et du management des organisations. C'est un enjeu de compétitivité, de pérennité et de responsabilité. Nous espérons que ce numéro vous apportera des éclairages utiles pour progresser sur ce chemin.

Bonne lecture à tous !

L'équipe éditoriale

Chers experts en résilience et gestion de crise,

Nous vous invitons à partager votre expertise dans notre magazine dédié à la résilience organisationnelle. C'est l'opportunité de mettre en lumière vos connaissances et d'inspirer nos lecteurs avec des stratégies innovantes sur des sujets clés tels que :

La continuité des activités - La gestion et la communication de crise - La reprise informatique post-incident - L'intelligence économique - La gestion des risques - La cybersécurité - ...

Pour participer, envoyez-nous un résumé de votre proposition d'article à **info@crise-resilience.com**.

Partagez vos retours d'expérience, vos analyses et vos conseils pratiques pour aider les organisations à renforcer leur résilience face aux crises. Vos perspectives uniques et approches novatrices intéresseront vivement notre lectorat de professionnels.

Rejoignez notre communauté d'experts et contribuez à développer une culture de résilience dans le monde de l'entreprise.

Nous avons hâte de collaborer avec vous pour offrir un contenu de qualité à nos lecteurs.

L'équipe éditoriale

Direction de la publication: A.Fournier
Correction: Véronique Cyr - **Création graphique:** Alfo65 - **Crédit photo:** FreePix – Dall-E 3 – MidJourney - **Édition:** Crise&Résilience- Québec (Qc), Canada
Nous contacter : info@crise-resilience.com

Sommaire

Numéro 7 – JUILLET 2024

Rejoignez-nous sur **LinkedIn**

Version flip en ligne sur

www.criseetresilience-magazine.com

Interview de Christophe Vanypre

Comment récupérer ses données perdues?

Interview

Christophe Vanypre

Directeur de Recoveo Software et de Recoveo

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

Découvrez les techniques de pointe utilisées pour sauver vos précieuses informations des pannes, des cyberattaques et même des sinistres.

Une interview passionnante qui lève le voile sur la récupération de données.

Interview Alexandre FOURNIER

Expert en gestion et simulation de crise

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

La perte de données est un cauchemar que redoutent toutes les entreprises. Que ce soit à cause d'une panne matérielle, d'une cyberattaque ou d'un sinistre, la récupération des données devient alors une priorité absolue.

Dans cette interview captivante, nous vous invitons à découvrir les coulisses de la récupération de données avec Christophe Vanypre, directeur de Recoveo Software et de Recoveo.

Spécialiste dans ce domaine depuis plus de huit ans, Christophe nous dévoile les techniques de pointe et les défis quotidiens de cette technologie méconnue, mais cruciale.

Q: Pouvez-vous nous présenter votre activité?

Christophe Vanypre : Recoveo est historiquement spécialisée dans la récupération de données depuis tout type de support informatique lorsque celles-ci sont devenues inaccessibles, que ce soit sur des disques durs, des serveurs, des systèmes flash, etc.

Nous sommes passés au fil du temps de connaissances mécaniques et informatiques à des connaissances en microélectronique pour pouvoir récupérer les données sur les disques SSD. Et depuis 2017, nous nous sommes penchés sur la récupération de données à la suite d'attaques par rançongiciel.

Aujourd'hui, Recoveo est la seule solution au paiement de la rançon lorsque toutes les données sont chiffrées après une cyberattaque.

Justement, quelle est votre méthode pour récupérer les données perdues à la suite d'une cyberattaque?

C.V. : Contrairement aux idées reçues, lors d'une attaque par rançongiciel, les données ne sont en réalité chiffrées qu'à hauteur de 5 à 20 % en moyenne.

Nos techniques consistent soit à contourner le chiffrement quand c'est possible, soit à réparer et à reconstruire les données chiffrées.

Pour cela, l'idéal est d'avoir une multitude de données, y compris des sauvegardes chiffrées, car tout n'est pas chiffré de la même façon au même endroit.

En ayant plusieurs supports, on peut reconstituer les données par petits morceaux, comme un puzzle, pour aboutir à un résultat fonctionnel.

Quels sont les principaux défis techniques que vous rencontrez?

C.V. : Concernant, la récupération de données traditionnelle, la miniaturisation des supports, le passage aux disques SSD et les mesures de sécurité mises en place par les constructeurs complexifient nos techniques.

Sur la partie cyberattaque, les hackers font constamment évoluer leurs méthodes de chiffrement. Notre défi est de nous adapter en permanence en fonction des particularités de chaque système du client et du mode opératoire des attaquants.

Mais plus on a de supports de données, plus on a de chances de pouvoir reconstruire une donnée valide.

"Contrairement aux idées reçues, lors d'une attaque par rançongiciel, les données ne sont en réalité chiffrées qu'à hauteur de 5 à 20 % en moyenne."

Christophe Vanypre

Combien de temps prend en moyenne une récupération de données?

C.V. : Cela dépend de l'urgence et de l'énergie qu'on y met. Pour une récupération classique sur disque dur, il faut compter environ une semaine. Mais nous avons des formules d'urgence où un ingénieur va se consacrer à 100 % à un dossier, ce qui permet d'aller beaucoup plus vite, en 24 h ou 48 h.

C'est souvent le cas lors de cyberattaques, où il y a une vraie urgence à récupérer les données. Il arrive même qu'on récupère les données avant que l'infrastructure du client ne soit réinstallée!

Quels conseils donneriez-vous à une entreprise qui perd ses données à la suite d'une cyberattaque?

C.V. : La première chose est de faire appel à une société de récupération de données expérimentée pour éviter toute mauvaise manipulation qui rendrait la récupération impossible par la suite.

Ensuite, il faut faire une copie des sauvegardes et des machines virtuelles chiffrées sur un support externe, car elles peuvent servir à la reconstruction.

Enfin, il faut bien choisir son prestataire en s'assurant de ses compétences spécifiques en récupération post rançongiciel, mais aussi de son indépendance et de sa capacité à garantir la souveraineté des données.

C'est un point crucial, car les données confiées peuvent être sensibles.

Justement, comment garantissez-vous cette souveraineté des données de vos clients?

C.V. : Chez Recoveo, nous avons fait le choix stratégique de nous développer pour atteindre une taille critique, financer notre R&D et être capables de traiter tous les types de supports et de pannes en interne, sans faire appel à la sous-traitance.

Nous travaillons sous législation française, nous sommes une entreprise 100 % française, et les données restent dans nos laboratoires en régions parisienne et lyonnaise, totalement déconnectés d'Internet.

C'est important, car il peut y avoir des conflits d'intérêts si les données sont confiées à des acteurs qui ne sont pas souverains.

Pour conclure, Christophe, comment voyez-vous évoluer votre expertise dans les années à venir?

C.V. : La donnée est devenue un enjeu de business majeur pour les entreprises. Sans données, une entreprise ne peut plus fonctionner. Donc le besoin de récupération en cas de perte, que ce soit à la suite d'une panne ou d'une cyberattaque, va continuer à se renforcer.

Cela va nécessiter de suivre les évolutions technologiques et de renforcer encore notre R&D pour être toujours en mesure de récupérer les données, avec des outils toujours plus pointus.

L'autre enjeu sera la protection de la souveraineté des données, qui va devenir un critère différenciant dans le choix d'un prestataire. Nous sommes armés pour répondre à ces deux défis.

Interview de Stéphane Vanypre par Alexandre Fournier

En savoir plus, visiter **www.recoveo.com**

Écouter l'interview de Stéphane

Cliquer sur l'image

PROTÉGEZ VOS DONNÉES

ne laissez pas vos données à la merci du hasard,

adoptez la MÉTHODE 3.2.1.1.0 !

3

COPIES DE DONNÉES

Ayez au moins trois copies de vos données pour éviter la perte d'informations.

2

TYPES DE SUPPORTS DIFFÉRENTS

Utilisez deux types de supports de stockage différents pour minimiser les risques de défaillance.

1

COPIE HORS SITE

Conservez une copie de vos données dans un emplacement différent pour les protéger contre les sinistres locaux.

1

COPIE HORS LIGNE

Gardez une copie de vos données déconnectée du réseau pour la protéger contre les cyberattaques.

0

ERREURS

Assurez-vous que vos sauvegardes sont vérifiables et sans erreurs pour garantir leur fiabilité.

SÉCURISEZ VOTRE FUTUR

La crise permanente à marche forcée pour les dirigeants des entreprises

La crise permanente et multiple devient la norme.

C’est le moment de s’adapter à des règles du jeu qui vont tendanciellement se durcir.

C’est aussi une façon de valoriser l’actif.

Par Vincent Balouet

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

Les crises deviennent plus nombreuses, plus variées et plus simultanées. Depuis la COVID, les directions générales se sont aussi transformées en cellules de crise permanentes, au risque de réagir trop tard face à des situations insuffisamment préparées ou anticipées. On doit pouvoir faire nettement mieux.

État permanent de crise

Depuis la crise dite « des gilets jaunes » en 2018 et, plus singulièrement, la COVID, les chefs d'entreprise ont pris à leur corps défendant l'habitude de gérer des crises en permanence, voire plusieurs crises à la fois.

Mouvements sociaux, pandémie, cyberattaques, inondations, sécheresses, risques sur les infrastructures électriques, contexte géopolitique préoccupant en Europe, au Proche-Orient et en Asie, terrorisme, instabilité outre-mer.

Ces réalités nécessitent que les sujets qui remontent en direction générale aient été convenablement triés et préparés afin de ne pas saturer de manière improductive les dirigeants d'entreprise, lesquels doivent aussi s'occuper de la marche normale de leurs affaires.

La quantité de signaux faibles et d'informations en amont est donc en très forte croissance, et la compréhension des enjeux majeurs du modèle économique de l'entreprise, les fonctions et les processus critiques sont autant de notions à posséder impérativement pour pouvoir effectuer ce tri.

Crises multisectorielles

Par ailleurs, la crise liée à une survenance simultanée de plusieurs crises de nature différente (par exemple une catastrophe climatique, une inondation ou une tempête et une cyberattaque simultanée) peut être rendue particulièrement délicate à régler du fait de l'annulation croisée des plans de continuité.

En effet, le travail à distance et l'utilisation renforcée des moyens numériques constitue un excellent plan B à de très nombreux types de crises, lequel devient inopérant en cas de cyberattaque simultanée.

La diversification des crises en nature et au niveau l'état de crise permanent et la possibilité de crises majeures simultanées renforcent donc la difficulté de l'exercice, et appellent à prendre le sujet de plus en plus sérieusement, avec des compétences renforcées et, de préférence, toujours un temps d'avance.

Conséquences environnementales

Devant nous, l'augmentation en fréquence et en gravité des catastrophes climatiques promises par le GIEC amènera inévitablement les dirigeants, avec l'augmentation des conditions et des coûts de l'assurance, à durcir l'entreprise face à ces risques.

Autrement dit, certaines activités devront déménager ou s'organiser autrement, loin du rivage, à proximité de sources d'énergie redondantes et fiables, sous une toiture renforcée, etc.

Dans le même temps, dans l'espace numérique, l'activité malveillante continue d'exploser et la très forte croissance des systèmes consacrés à l'utilisation de l'intelligence artificielle va très certainement conduire à une situation de plus en plus compliquée et volumineuse.

La gestion des crises simultanées et complexes devient donc tendanciellement un élément stratégique déterminant, qui contribue par ailleurs à la valorisation des actifs de l'entreprise.

Au moment des fusions-acquisitions, une entreprise bunker vaut toujours plus qu'une entreprise passoire.

Modèle d'affaires affecté

Ce contexte amène donc les dirigeants à réfléchir à l'évolution du modèle économique de la prévention, à sa contribution à l'actif de l'entreprise et, par conséquent, à son statut juridique et à sa fiscalité.

De même, dans les parcours scolaires, la gestion de crises en entreprise devra nécessairement être plus présente, voire rendue obligatoire, de même que les fondamentaux en sciences et en gestion aujourd'hui, qu'il s'agisse de futurs dirigeants du privé ou ceux promis à une carrière publique.

À plus court terme, les dirigeants des entreprises ont intérêt, d'une part, à renforcer la fonction « continuité » et ainsi à se libérer d'une part importante de la gestion des crises multiples ne relevant pas réellement du niveau de la direction générale et, d'autre part, à **mettre en place une anticipation raisonnable des crises à venir** permettant de déclencher en amont certaines actions très économiques en temps et en énergie afin de s'affranchir du syndrome de la copie blanche.

À plus court terme,
les dirigeants des entreprises ont intérêt, à renforcer la fonction « continuité »

Mondialisation et flexibilité

Dans le contexte actuel marqué par une situation géopolitique internationale plus instable, la multiplication des cyberattaques, les prémices d'une pandémie potentielle venant des élevages bovins, sans oublier, bien entendu, la dérive climatique et ses multiples conséquences, **il n'est pas interdit d'installer les bons réflexes d'une hygiène-continuité en maintenant un système d'information souple et utilisable à distance quoi qu'il arrive, des cadres et des dirigeants préparés grâce à des exercices sans doute plus réguliers et plus pertinents, et une communication plus fluide** qui vend aussi la préparation aux risques majeurs et multiples non pas comme une peur, mais comme un actif de l'entreprise.

Préparation et paix relative d'esprit

Dans un monde qui restera concurrentiel, un rapport apaisé aux risques majeurs et à la gestion de crises permet de libérer du temps, de mieux investir, de mieux recruter aussi.

Une entreprise bien préparée et performante en gestion de crises multiples permet donc de mieux s'entourer, d'établir et d'entretenir un haut niveau de confiance avec ses fournisseurs et ses clients et de projeter une image de confiance maîtrisée.

Les entreprises, mais aussi les administrations, les collectivités et les associations, n'auront de toute façon pas d'autre choix que de prendre le risque de devoir lancer ces mêmes actions en urgence et moins adroitement au moment même de la crise.

L'anticipation est la clé. La gestion de crises est pour beaucoup une affaire de bon sens et de préparation raisonnable. Le renforcement de ces capacités est un actif facile à valoriser et un puissant générateur de confiance.

Vincent Balouet

MAITRISE DES CRISES

Vincent Balouet intervient auprès des dirigeants des grandes entreprises depuis plus de 30 ans. Il a été à l'origine de la mobilisation française lors de la crise Y2K et a été appelé par le gouvernement à fortifier la préparation générale des entreprises. Il dirige aujourd'hui Maîtrise des crises.

www.maitrisedescrises.com

4 recommandations pour ne pas rester immobile

1 : **Anticipez les crises** qui arrivent grâce à une veille ciblée et à une cellule d'anticipation pluridisciplinaire dont la première qualité sera le bon sens.

2 : **Construisez un corpus de fiches réflexes** simples permettant de bien lancer les premières actions en cas d'urgence.

3 : **Faites des exercices réguliers**, y compris en direction générale, avec une forme accélérée.

4 : **Vendez la gestion de crises** comme un actif, en interne et en externe, capitalisez sur la confiance.

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

Pour en savoir plus, cliquer sur la vidéo.

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

ABONNEZ-VOUS Gratuitement

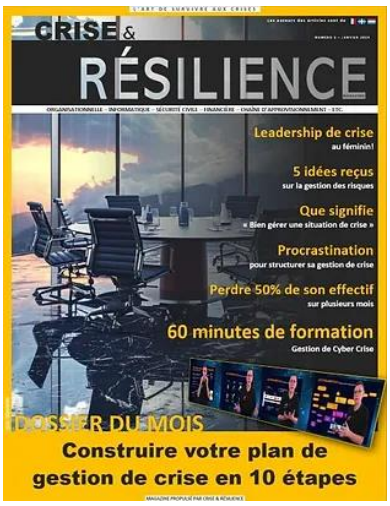
TRIMESTRIEL – JANVIER – AVRIL – JUILLET – OCTOBRE

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

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

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

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



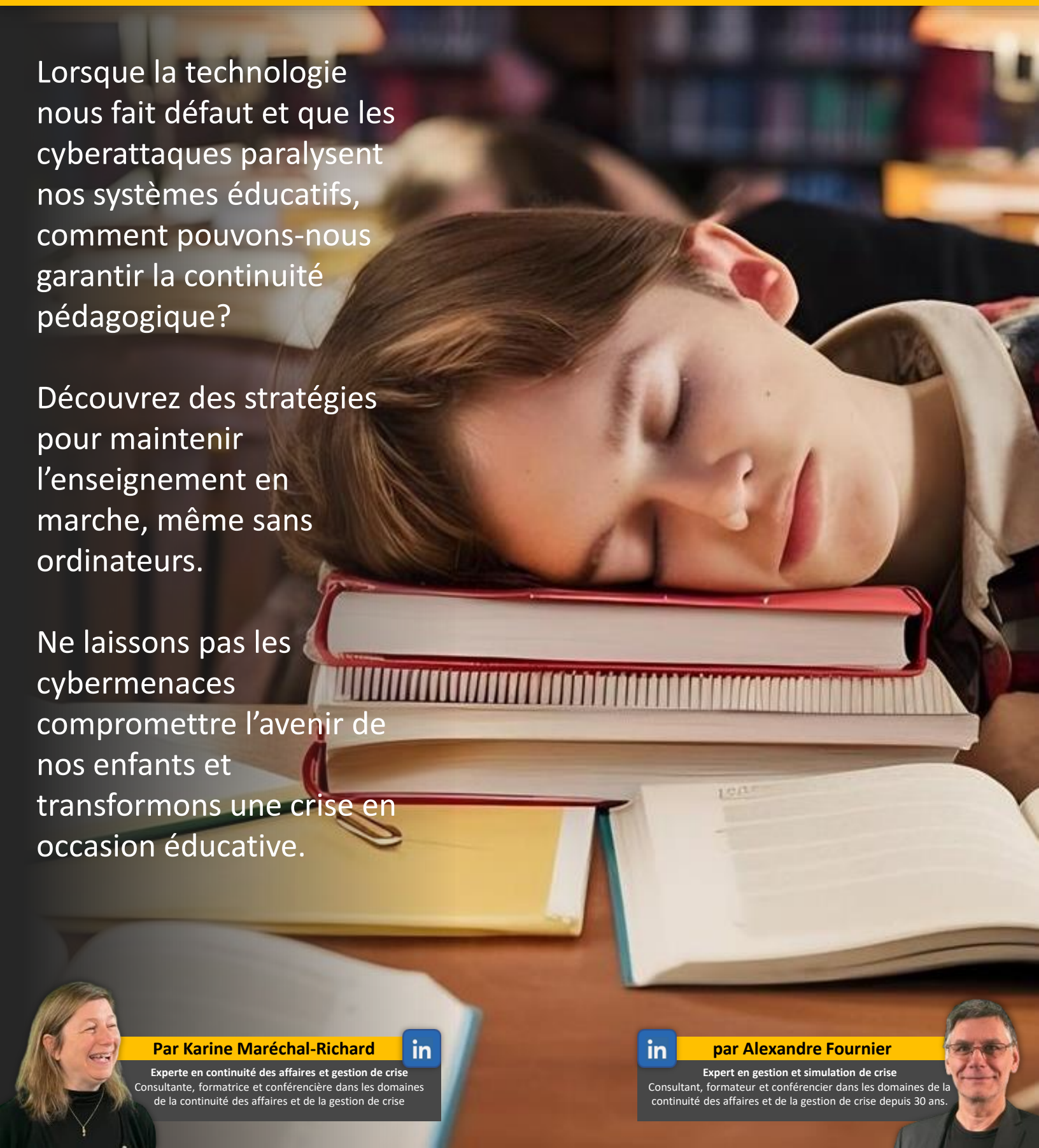
Abonnez-vous sur www.criseetresilience-magazine.com

La chaîne YouTube Crise & Résilience

Des conférences et formations gratuites

Des interviews d'experts :

Cyberattaque : Continuer l'enseignement sans informatique!



Lorsque la technologie nous fait défaut et que les cyberattaques paralysent nos systèmes éducatifs, comment pouvons-nous garantir la continuité pédagogique?

Découvrez des stratégies pour maintenir l'enseignement en marche, même sans ordinateurs.

Ne laissons pas les cybermenaces compromettre l'avenir de nos enfants et transformons une crise en occasion éducative.

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

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'informatique est devenue omniprésente à tous les niveaux de l'éducation, et les cyberattaques représentent une menace croissante pour les établissements scolaires et universitaires.

Les cyberattaques peuvent paralyser les systèmes informatiques, entraînant de graves perturbations dans l'enseignement et dans la gestion administrative.

L'indisponibilité des supports numériques, tels que les cours en ligne et les ressources pédagogiques, complique la préparation et la diffusion des leçons.

La communication et la coordination entre enseignants, administrateurs et étudiants deviennent difficiles, affectant l'organisation des cours et le partage d'informations cruciales.

De plus, les complications dans les évaluations et le suivi des progrès peuvent démotiver les étudiants et retarder leur parcours scolaire.

Je vous propose, dans cet article, de revenir sur quelques impacts les plus courants et de vous proposer quelques pistes afin de limiter ces conséquences et de maintenir les activités d'enseignement sans informatique à minima.

MISE EN GRADE… Certaines pistes pourront vous paraître évidentes et, pourtant, elles sont de plus en plus délaissées au profit de la dématérialisation de l'enseignement, ce qui entraîne une nouvelle dépendance envers des outils informatiques.

1- Impacts des cyberattaques sur l'éducation

Lors d'une cyberattaque dans les établissements scolaires, on constate généralement les impacts suivants :

Absence de supports numériques : le matériel pédagogique est de plus en plus hébergé de façon centralisée pour diverses raisons, sur des supports numériques qui deviennent inaccessibles lors d'une cyberattaque. Les cours, les ressources pédagogiques et les évaluations sont alors indisponibles, compliquant la préparation et la diffusion des leçons pour les enseignants et limitant l'accès des élèves et des étudiants aux matériels nécessaires.

Perturbation de la communication et de la coordination : les outils de communication en ligne, tels que les courriels et les plateformes collaboratives, sont devenus essentiels pour la gestion quotidienne des établissements scolaires. Lors d'une cyberattaque, ceux-ci peuvent devenir inaccessibles, perturbant ainsi la collaboration entre enseignants, administrateurs et étudiants et rendant difficiles l'organisation des cours et le partage d'informations importantes.

Complications dans les évaluations et le suivi des progrès : les systèmes de gestion des notes et des évaluations peuvent aussi être indisponibles pour diverses raisons liées directement ou non à la cyberattaque. Leur indisponibilité complique le suivi des performances, la gestion des évaluations et la communication des résultats, entraînant des retards et pouvant affecter la motivation des étudiants et des élèves. Cette indisponibilité peut avoir un impact immédiat ou à moyen terme pour les inscriptions dans les universités en provoquant, par exemple, un stress supplémentaire sur le système éducatif et les étudiants eux-mêmes.

Hyper dépendance aux technologies et nécessité d'adaptation : de plus en plus, les méthodes d'enseignement modernes reposent fortement sur les technologies numériques.

Une cyberattaque désactivant ces technologies oblige les enseignants à adapter rapidement leurs approches pédagogiques, souvent en recourant à des méthodes traditionnelles pour lesquelles ils ne sont pas toujours organisés en raison de la dématérialisation des cours.

Ces quelques impacts – il y en a bien sûr d'autres – soulignent l'importance de la préparation et de la mise en place de solutions de mitigation dont l'objectif est de minimiser le plus possible les perturbations et de permettre une continuité pédagogique la plus optimale possible.

2- Stratégies de résilience pédagogique

Pour faire face à ces défis, il est essentiel de planifier et de mettre en place des stratégies en collaboration avec le corps professoral et le personnel administratif.

Ces stratégies doivent être préparées, de préférence avant la survenue d'une crise, afin de réduire les situations de stress et de panique au moment de la crise.

Méthodes d'enseignement traditionnelles : maintenir les méthodes d'enseignement traditionnelles en présentiel, telles que les cours magistraux, les discussions en classe et les présentations orales, assure la continuité pédagogique en cas d'interruption des technologies numériques, notamment s'il y a rupture des cours à distance.

Ces approches favorisent une interaction directe et personnelle entre les enseignants et les étudiants. De plus, les ateliers pratiques et les travaux de groupe encouragent la collaboration et l'apprentissage par l'expérience, s'adaptant facilement à un environnement sans technologie.

Cela peut paraître évident et déjà appliqué pour les cours donnés en présentiel. Et en même temps, la dématérialisation tend à réduire cette stratégie au profit de cours en ligne et principalement dématérialisés.

Ressources pédagogiques traditionnelles : utiliser des livres, des cahiers et des supports imprimés est essentiel pour continuer l'enseignement sans dépendre des technologies numériques. Les bibliothèques scolaires et universitaires peuvent fournir d'autres types de ressources pédagogiques.

La distribution régulière de photocopies de documents importants permettra aux étudiants de continuer à étudier et à compléter leurs devoirs même en l'absence d'un accès centralisé au système informatique et/ou à Internet.

De plus, le fait d'avoir une copie de l'ensemble des cours (à jour) sur l'ordinateur ou sur une clé USB permettra à l'enseignant d'être autonome pour la diffusion des cours en classe.

Cela permet de pallier l'indisponibilité du système informatique centralisé qui héberge les cours.

Communication et coordination sans technologie : en l'absence d'outils de communication numériques, les établissements doivent mettre en place de nouvelles méthodes pour maintenir la communication et la coordination. Voici quelque piste de solution :

- Utiliser les téléphones pour les appels et les messages permet de rester en contact avec le personnel et les étudiants;
- Installer des tableaux d'affichage pour diffuser les informations importantes et les mises à jour quotidiennes assure une communication fluide malgré l'absence de technologies numériques au sein de l'école;
- Désigner des « ambassadeurs étudiants » dans chaque classe ou groupe chargés de relayer les informations à leurs camarades et de faire remonter les questions ou les préoccupations aux enseignants favorise une communication bidirectionnelle et implique les étudiants dans le processus;
- Utiliser les médias sociaux permet de conserver le contact avec les étudiants. La possibilité d'utiliser la radio locale ou la radio étudiante peut aussi être envisagée.

Bien sûr, vous pouvez aussi préparer des solutions de messagerie de secours pour le personnel essentiel.

Évaluations et suivi des progrès : en l'absence de systèmes numériques, les évaluations peuvent se faire à l'aide de méthodes traditionnelles, comme les examens sur papier en présentiel et les évaluations orales. Les enseignants peuvent donner des retours directs et personnalisés aux étudiants pour les guider dans leur apprentissage, permettant de maintenir un suivi régulier des progrès.

Partenariats et soutien communautaire : les établissements scolaires ne doivent pas rester isolés dans leur lutte pour maintenir la continuité pédagogique. Établir des partenariats solides avec d'autres établissements et mobiliser le soutien de la communauté locale sont des stratégies qui permettent de renforcer la résilience face aux interruptions technologiques. Voici quelques pistes à explorer entre établissements scolaires :

- Créer un réseau d'entraide pour faire connaître les informations sur les cyberattaques et, surtout, les solutions mises en œuvre.
- Mutualiser les ressources pédagogiques pour maintenir la continuité des enseignements.
- Organiser des formations communes sur la gestion de crise et la pédagogie sans technologie.
- Partager les infrastructures pour surmonter les perturbations matérielles.

Voici d'autres pistes avec la communauté locale :

- Impliquer les parents d'élèves en les informant et en encourageant leur participation active.
- Collaborer avec les associations locales pour obtenir des locaux de remplacement et du soutien.
- Solliciter l'appui des entreprises pour parrainer des projets et fournir du matériel de secours.
- Travailler avec les autorités locales pour assurer la sécurité des élèves et des étudiants et obtenir des ressources supplémentaires, par exemple en cas d'indisponibilité des systèmes de vidéosurveillance et de domotique.

Formation et sensibilisation : la formation régulière du personnel et des enseignants sur les protocoles de crise et la gestion des interruptions technologiques renforce la résilience de l'établissement. Une sensibilisation accrue à ces enjeux permet de minimiser les impacts sur l'apprentissage. De plus, une mise en situation annuelle pourrait permettre de valider les plans de continuité pédagogique.

Plan de reprise informatique : pour assurer la reprise rapide et viable de l'enseignement sous forme numérique post-cyberattaque, il est essentiel de mettre en place des sauvegardes régulières des données critiques sur des supports externes et non connectés.

Il pourrait aussi y avoir des systèmes de secours unidirectionnels qui permettraient d'héberger localement :

- Les copies des cours, les exercices et les ressources pédagogiques essentielles;
- Les notes et les suivis des étudiants;
- Les copies d'examens en cours;
- Tout autre support essentiel à la mission.

Cette dernière stratégie peut permettre le maintien des services éducatifs numériques à minima, malgré les interruptions technologiques centrales.

S'entraîner et actualiser ses plans : s'entraîner régulièrement et actualiser les plans de continuité pédagogique est essentiel pour s'assurer que les établissements scolaires peuvent répondre efficacement aux cyberattaques. En simulant des scénarios de crise, et en actualisant régulièrement les procédures, les écoles, les collèges et les universités peuvent renforcer leur résilience et maintenir la continuité de leur enseignement même en cas de crise technologique.

Les cyberattaques constituent une menace grave pour les établissements scolaires, perturbant l'enseignement, la communication et les évaluations. Pour garantir la continuité pédagogique, il est crucial de maintenir des méthodes d'enseignement sans technologie, d'utiliser des ressources pédagogiques traditionnelles (papier, crayon, tableau) et de mettre en place des moyens de communication non numériques. Sensibiliser régulièrement le personnel à la résilience hors technologie et conserver des sauvegardes de données sécurisées et accessibles en tout temps sont des mesures indispensables.

La clé de la résilience réside dans l'entraînement régulier et l'actualisation des plans de continuité. En simulant des crises et en adaptant les procédures, les établissements peuvent s'assurer que l'éducation des élèves et des étudiants n'est jamais compromise, même face aux défis technologiques. Cette résilience, construite sur la préparation, la flexibilité et la détermination, garantit que l'enseignement poursuivent leur mission, même dans les moments les plus sombres.

Karine Maréchal-Richard & Alexandre Fournier

Nous accompagnons les organisations de l'éducation à travers la mise en place de plan de gestion de crise, de continuité des affaires, de reprise informatique et de simulation de crise. Nous avons déjà accompagné plus d'une cinquantaine d'établissements scolaire et universitaire.

www.crise-resilience.com

Participez à cette conférence spéciale pour le domaine de l'enseignement.

Préparez l'imprévu!
8 astuces pour une résilience pédagogique renforcée

Voici 8 astuces pour renforcer la résilience pédagogique et être prêt à affronter l'imprévu :

Créez votre « trousse de survie pédagogique » : ayez toujours sous la main des versions imprimées de vos cours, des manuels et des exercices. Encouragez vos élèves ou vos étudiants à conserver une copie papier de leurs notes et de leurs travaux importants. Avec votre trousse, vous serez parés pour enseigner, même sans technologie!

Établissez un système de communication de secours : échangez les numéros de téléphone avec vos collègues, et prévoyez un point de ralliement physique pour afficher les informations importantes. Désignez des « ambassadeurs étudiants » pour relayer les messages clés. Vous maintiendrez ainsi le contact, même sans courriels!

Transformez vos évaluations (enseignement à distance) : optez pour des examens sur papier et en présentiel et des présentations orales. Préparez des sujets adaptés et des grilles d'évaluation claires. Donnez des rétroactions individuelles pour maintenir la motivation. Vos étudiants continueront ainsi à progresser, même sans plateforme en ligne!

Tissez des liens avec votre écosystème local : nouez des partenariats avec les établissements voisins, les associations et les entreprises locales. Faites connaître vos ressources, vos bonnes pratiques et vos solutions innovantes. Ensemble, vous serez plus forts pour surmonter les défis!

Formez-vous et impliquez-vous : participez activement aux formations sur la cyberrésilience proposées par votre établissement. Soyez une force de proposition pour améliorer les plans de continuité. Votre expertise de terrain est précieuse pour renforcer la résilience collective!

Sauvegardez l'essentiel : effectuez régulièrement des sauvegardes de vos données critiques sur des supports externes sécurisés. Prévoyez des systèmes de secours pour maintenir l'accès aux ressources pédagogiques essentielles. Vous pourrez ainsi récupérer rapidement vos contenus en cas de besoin!

Entraînez-vous et adaptez-vous : simulez régulièrement des scénarios de crise pour tester vos procédures. Actualisez vos plans de continuité en fonction des retours d'expérience. En vous entraînant et en vous adaptant, vous serez toujours prêt à assurer la continuité pédagogique, quoi qu'il arrive!

Pensez aux élèves bénéficiant de programmes adaptés : réfléchissez à des méthodes d'enseignement adaptées aux élèves ayant des besoins particuliers, et assurez-vous qu'ils disposent de ressources adéquates même en l'absence d'outils informatiques.

TÉLÉCHARGER GRATUITEMENT

15 AFFICHES DE SENSIBILISATION

A TÉLÉCHARGER SUR WWW.CRISE-RESILIENCE.COM

Télécharger ici

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

Comment construire un exercice de gestion de crise

Un exercice de gestion de crise bien conçu permet non seulement de tester la résilience de l'organisation, mais aussi de renforcer sa préparation face à des scénarios divers allant des catastrophes naturelles aux cyberattaques.

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

Dans un monde professionnel en constante évolution où les risques et les incertitudes sont omniprésents, la capacité d'une entreprise à rebondir face à des événements majeurs est essentielle.

Un exercice de gestion de crise bien conçu permet non seulement de tester la résilience de l'organisation, mais aussi de renforcer sa préparation face à des scénarios divers allant des catastrophes naturelles aux cyberattaques.

Pour la rédaction de ce dossier, nous nous sommes appuyés sur une feuille de route que nous utilisons chez nos clients pour réaliser des exercices de simulation de crise.

Cette feuille de route, alignée sur les meilleures pratiques en vigueur, puise aussi sa force dans plusieurs années d'expérience multidisciplinaire dans le domaine de la gestion de crise et la simulation.

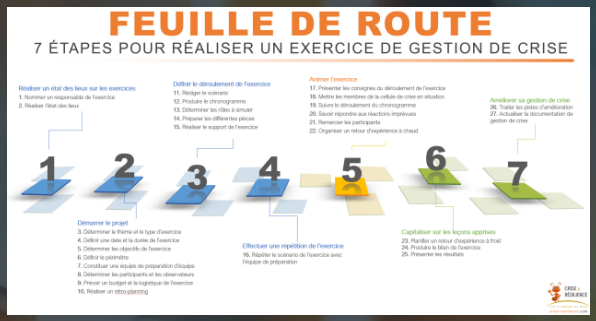
L'objectif de ce dossier est de proposer un guide structuré pour élaborer des exercices de gestion de crise robuste et efficace de A à Z.

Le document est structuré en trois phases :

- la préparation d'un exercice de gestion de crise,
- son exécution,
- et les apprentissages ainsi que l'amélioration continue des plans.

Chaque phase est subdivisée en étapes clés détaillées et explicitées pour faciliter votre navigation.

En suivant ce guide, vous serez en mesure de concevoir et de réaliser des exercices de gestion de crise qui amélioreront la résilience et la préparation de votre organisation face à des événements imprévus.



FEUILLE D

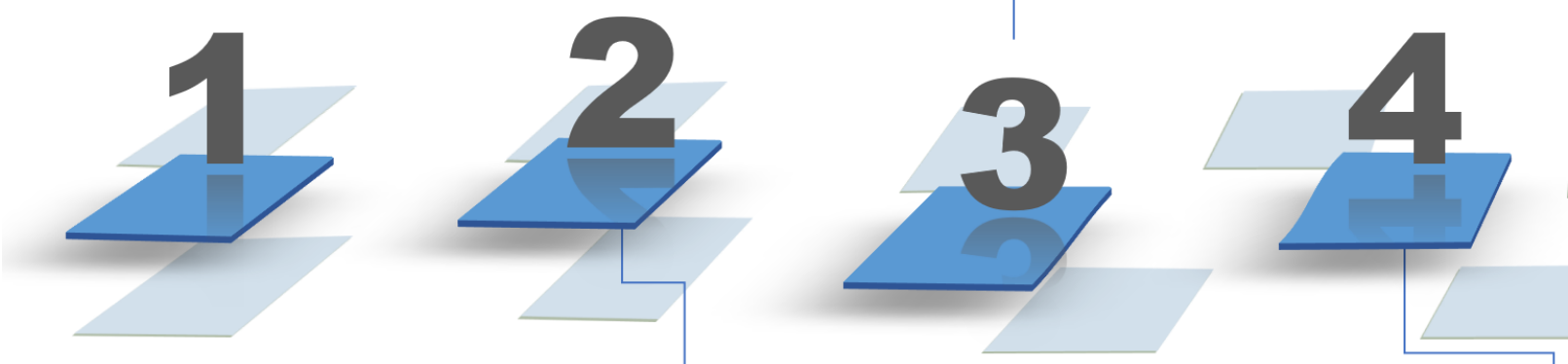
7 ÉTAPES POUR RÉALISER UN E

Réaliser un état des lieux sur les exercices

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

Définir le déroulement de l'exercice

11. Rédiger le scénario
12. Produire le chronogramme
13. Déterminer les rôles à simuler
14. Préparer les différentes pièces
15. Réaliser le support de l'exercice



Démarrer le projet

3. Déterminer le thème et le type d'exercice
4. Définir une date et la durée de l'exercice
5. Déterminer les objectifs de l'exercice
6. Définir le périmètre
7. Constituer une équipe de préparation d'équipe
8. Déterminer les participants et les observateurs
9. Prévoir un budget et la logistique de l'exercice
10. Réaliser un rétro-planning

Effectuer une répétiti

16. Répéter le scénario
l'équipe de préparation

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

DE ROUTE

XERCICE DE GESTION DE CRISE

Animer l'exercice

17. Présenter les consignes du déroulement de l'exercice
18. Mettre les membres de la cellule de crise en situation
19. Suivre le déroulement du chronogramme
20. Savoir répondre aux réactions imprévues
21. Remercier les participants
22. Organiser un retour d'expérience à chaud

Améliorer sa gestion de crise

26. Traiter les pistes d'amélioration
27. Actualiser la documentation de gestion de crise

on de l'exercice

de l'exercice avec

Capitaliser sur les leçons apprises

23. Planifier un retour d'expérience à froid
24. Produire le bilan de l'exercice
25. Présenter les résultats

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

PHASE 1 – PRÉPARATION DE L'EXERCICE

La phase de préparation est la pierre angulaire de tout exercice de gestion de crise. Elle définit les objectifs, les moyens et le cadre de l'exercice, assurant ainsi sa pertinence et son efficacité. Une préparation rigoureuse transforme un simple exercice en un test réaliste et puissant des capacités de l'organisation à répondre aux crises.

Cette phase comprend des activités essentielles : nommer un responsable, planifier les activités et les ressources, définir les scénarios, sélectionner les participants et coordonner la logistique. Chaque détail compte. Investir du temps et des efforts dans cette préparation assure un déroulement fluide et productif, créant des opportunités précieuses d'apprentissage et d'amélioration continue. Dans cette section, nous décrirons chaque activité de la préparation avec des conseils pratiques et des recommandations pour garantir une préparation exhaustive et rigoureuse.

Étape 1 : Réaliser un état des lieux des exercices

L'évaluation des exercices précédemment réalisés, des procédures actuelles et des ressources disponibles est cruciale pour orienter la préparation du prochain exercice de gestion de crise.

Cette analyse initiale permet de capitaliser sur les expériences passées, d'identifier les lacunes et d'optimiser les plans existants. En établissant une base solide, cette étape assure que toutes les actions futures seront alignées avec les besoins réels de l'organisation et les meilleures pratiques en matière de gestion de crise, garantissant ainsi une préparation robuste et efficace.

Activité 1. Nommer un responsable de l'exercice

Avant de débuter l'état des lieux, il est impératif de nommer un responsable qui coordonnera toutes les étapes de la préparation et de l'exécution de l'exercice de gestion de crise.

Ce responsable, connu sous le nom de responsable du plan de continuité des activités (RPCA), a pour mission d'organiser des exercices de gestion de crise dans le cadre de ses responsabilités.

Il jouera un rôle central en assurant une communication fluide entre les équipes et en veillant à ce que chaque membre comprenne ses responsabilités et les attentes. De plus, il sera responsable de la gestion efficace des ressources nécessaires, qu'il s'agisse de matériels, de locaux ou de personnel.

Son rôle inclura également la supervision rigoureuse du respect des échéances et la résolution rapide des problèmes pouvant survenir, garantissant ainsi que l'exercice se déroule de manière fluide et productive.

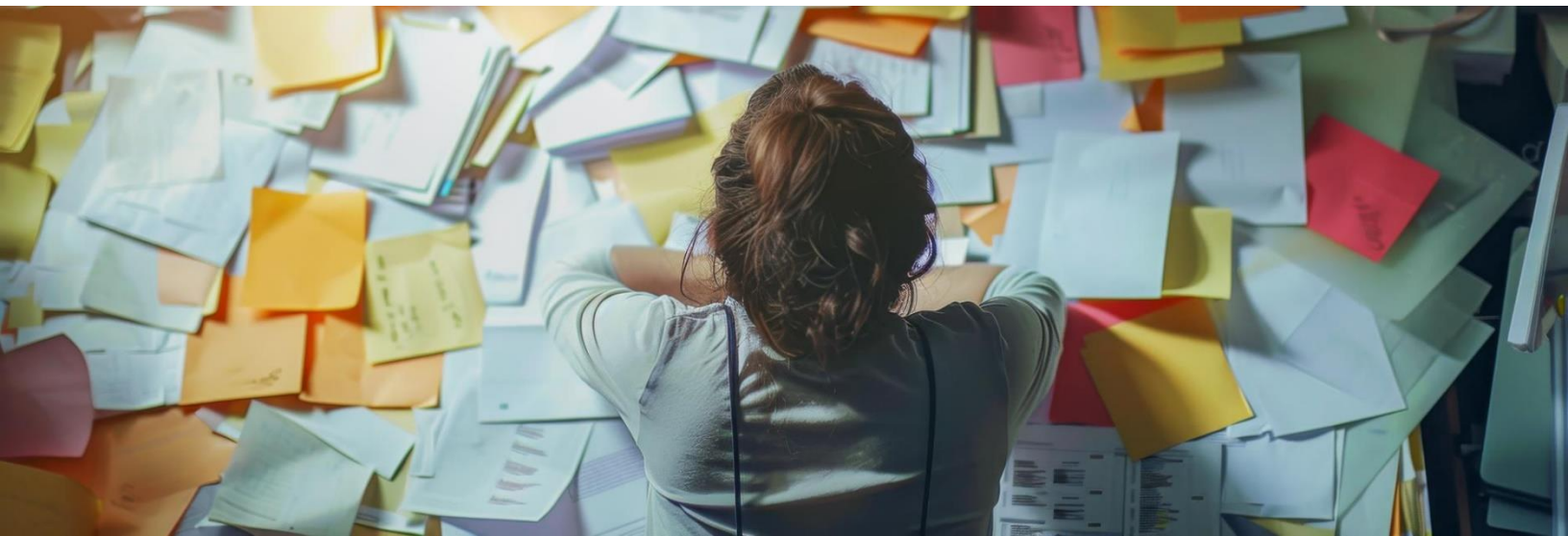
Activité 2. Réaliser l'état des lieux

La première étape dans la préparation d'un exercice de gestion de crise consiste à réaliser un état des lieux des exercices précédemment réalisés.

Cette analyse permet de dresser un tableau précis des forces et des faiblesses de l'organisation en matière de gestion de crise et de déterminer sa maturité en matière d'exercice.

En passant en revue les bilans des exercices passés, on peut identifier les réussites et les points à améliorer, ce qui offre une perspective claire sur le niveau de préparation actuel de l'organisation. La collecte de retours d'expérience (RETEX) des participants joue également un rôle clé, offrant des perspectives précieuses sur les aspects opérationnels ayant bien fonctionné et ceux nécessitant des ajustements.

En menant cette évaluation approfondie, l'organisation peut établir une base solide pour les actions futures en capitalisant sur les forces existantes et en remédiant proactivement aux faiblesses identifiées, tout en mesurant précisément sa maturité en matière d'exercice de gestion de crise.



Étape 2 : Démarrer le projet

Cette étape consiste à établir les fondations de l'exercice, incluant le choix du thème, la définition des objectifs et la constitution de l'équipe de préparation. Ces éléments fondamentaux sont essentiels pour structurer l'exercice de manière cohérente et garantir une compréhension claire des rôles et responsabilités de chacun.

Le choix d'un thème pertinent permet de simuler des scénarios réalistes, tandis que des objectifs bien définis orientent les actions et les évaluations.

La formation d'une équipe de préparation dédiée assure une coordination efficace et une mise en œuvre fluide de l'exercice.

Activité 3. Déterminer le thème et le type d'exercice

Choisir le thème et le type d'exercice est une étape fondamentale dans la préparation d'un exercice de gestion de crise. Cette décision influence non seulement le réalisme et la pertinence de l'exercice, mais aussi la manière dont les participants vont interagir et répondre aux situations simulées.

Pour préparer un exercice de gestion de crise efficace, il est essentiel d'identifier les risques les plus significatifs et prioritaires pour l'organisation. Ces risques peuvent inclure les catastrophes naturelles, les cyberattaques, les incidents industriels, les crises sanitaires ou les perturbations logistiques.

Les thèmes de l'exercice doivent refléter ces risques identifiés et être directement applicables aux opérations de l'organisation. Voici quelques exemples de thèmes pertinents : séisme, inondations, crise du verglas, cyberattaque avec fuite de données, explosion industrielle, épidémie, et bien d'autres encore.

Il existe différents types d'exercices, et le choix du type approprié dépendra de la maturité de l'organisation.

- **Exercice de table (Table-top) :** cet exercice est une discussion guidée visant à évaluer les plans et procédures de l'organisation. C'est le type d'exercice idéal pour commencer si vous n'en avez jamais réalisé auparavant. Il permet aux participants de se familiariser avec les plans et outils développés et identifie des solutions à des problématiques spécifiques, tout en réduisant le temps de préparation et de réalisation. Cependant, il ne teste pas un processus de gestion de crise complet ni les interactions avec tous les intervenants potentiels, contrairement à un exercice de simulation de crise complet.
- **Les tests :** ces exercices sont une étape incontournable pour avoir un plan de gestion de crise ou de continuité des affaires opérationnel et être prêt le jour « J ». Ils désignent un mécanisme de contrôle régulier des systèmes informatiques et de télécommunication impliquant un résultat d'échec ou de succès (cela fonctionne ou non). Que ce soit de petits tests ou des contrôles de grande envergure, il est conseillé de les planifier. Quant à la durée du test, elle varie selon l'objectif de l'exercice et du périmètre. Cet exercice est réalisé en utilisant les équipements du site de relève et la documentation liée à la reprise.
- **Simulation :** une simulation immersive en temps réel consiste à réagir à une crise simulée, offrant un haut degré de réalisme et permettant une évaluation approfondie des capacités opérationnelles. Ce type d'exercice reproduit une crise réaliste, mais fictive, telle qu'une cyberattaque, une destruction de site ou encore une médiatisation négative, et exécute les procédures selon un périmètre prédéfini.
- **Exercice à grande échelle :** cet exercice est conçu autour d'un scénario concret où les participants sont placés dans des circonstances semblables à celles d'un sinistre réel. La seule différence entre un exercice simulé et celui de grandeur réelle est la taille du périmètre. Dans un exercice à grande échelle, c'est toute l'organisation qui peut être impliquée ainsi que d'autre partenaires extérieurs, contrairement à une simulation où seule une petite partie de l'organisation est testée. Cet exercice est très intéressant à mettre en place, mais cela nécessite une grande maturité dans les plans et procédures de continuité. De plus, cet exercice est très coûteux.
- **Bascule réelle :** cet exercice permet de basculer le site de production sur le site de secours, qui devient alors le site de production pendant une certaine période. Cette manipulation doit être transparente pour les utilisateurs. Cet exercice permet de valider toutes les procédures de reprise informatique.

Activité 4. Définir une date et la durée de l'exercice

Définir une date et une durée pour l'exercice de gestion de crise est essentiel pour assurer son succès. La sélection de la date doit tenir compte de la disponibilité des participants, des partenaires externes et du calendrier des activités de l'organisation. Il est également important de choisir une période qui correspond à la saisonnalité des risques identifiés pour un scénario réaliste. L'exercice est dit « planifié » lorsque la date de l'exercice est connue par les participants.

Pour plus de réalisme, la date de l'exercice peut être inconnue des participants ; dans ce cas, c'est un exercice « surprise ». Le choix entre une simulation planifiée ou surprise dépendra du niveau de maturité de l'organisation et des objectifs fixés. Il est fortement recommandé de prévoir une seconde date en cas d'imprévu afin d'assurer que l'exercice puisse se dérouler sans interruption.

La durée de l'exercice doit refléter la complexité du scénario et les objectifs. Il est crucial de trouver un équilibre entre une simulation réaliste et la praticité afin de garantir une expérience d'apprentissage efficace et engageante pour tous les participants.

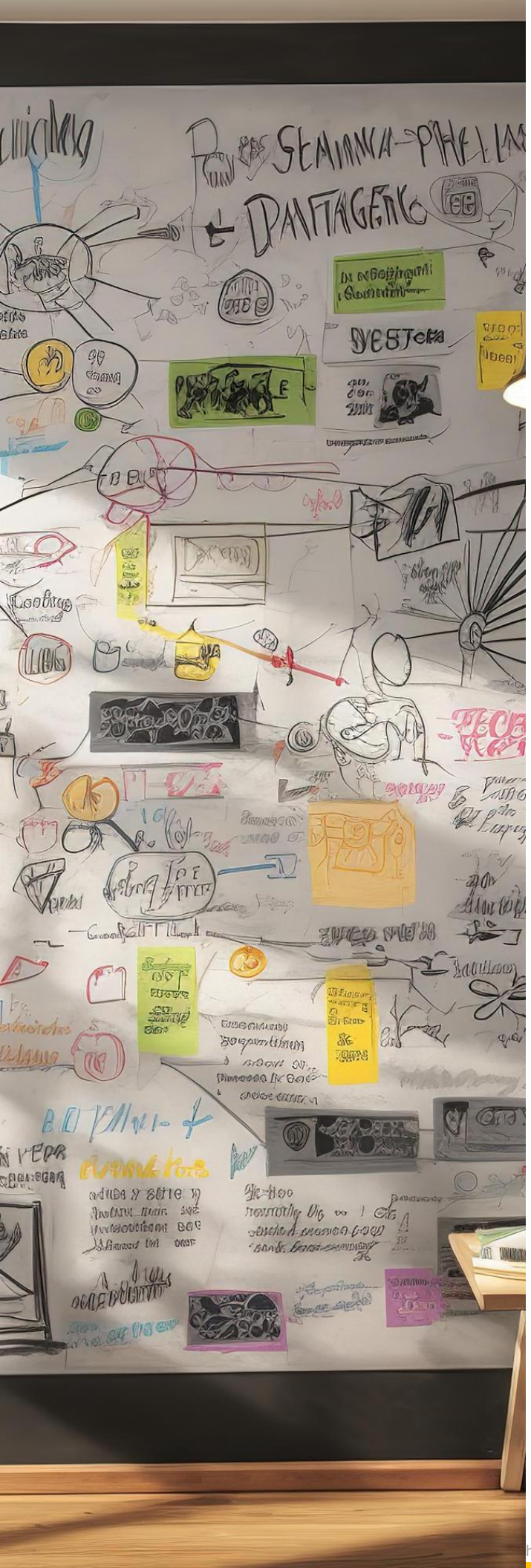
La durée doit être proportionnelle à la complexité du scénario choisi. Un scénario plus complexe nécessitera plus de temps pour être exécuté correctement et pour permettre aux participants de répondre de manière adéquate aux divers défis posés.

- **Scénarios simples :** les exercices portant sur des incidents mineurs ou des procédures spécifiques peuvent être plus courts, allant de quelques heures à une demi-journée.
- **Scénarios complexes :** les exercices couvrant des crises majeures impliquant plusieurs services, agences ou entités peuvent nécessiter une durée plus longue, souvent sur une journée entière voire plusieurs jours.

Activité 5. Déterminer les objectifs de l'exercice

Déterminer les objectifs de l'exercice est une étape cruciale dans la planification d'un exercice de gestion de crise. Cette phase établit la fondation sur laquelle tout l'exercice sera construit, influençant directement son efficacité et sa pertinence. Lors de cette planification, il est essentiel de distinguer les objectifs généraux des objectifs spécifiques. Cette distinction permet de structurer l'exercice de manière optimale, en s'assurant que les objectifs sont à la fois globaux et spécifiques, ce qui contribue à une préparation plus précise et à une évaluation plus rigoureuse des résultats.

- **Objectifs généraux :** ce sont des déclarations larges et globales qui décrivent les résultats attendus de l'exercice dans son ensemble. Ils fournissent une orientation stratégique et définissent l'intention principale derrière l'exercice, comme tester l'efficacité globale du plan de gestion de crise de l'organisation afin de repérer les points forts et les domaines à améliorer.
- **Objectifs spécifiques :** ce sont des déclarations détaillées et précises qui décrivent des résultats mesurables et concrets. Ils découlent des objectifs généraux et permettent de se concentrer sur des aspects particuliers de la gestion de crise. Par exemple, évaluer la rapidité et l'efficacité des procédures d'évacuation des bâtiments en mesurant le temps nécessaire pour évacuer en toute sécurité ou tester la capacité de l'équipe IT à détecter et neutraliser une cyberattaque en chronométrant le temps de réaction et la résolution de l'incident.



Activité 6. Définir le périmètre

Définir le périmètre de l'exercice est une étape essentielle pour garantir que l'exercice de gestion de crise soit bien structuré et ciblé.

Le périmètre délimite les frontières de l'exercice, précisant ce qui sera inclus et ce qui sera exclu. Cela permet de concentrer les ressources et les efforts sur les aspects les plus critiques et pertinents pour l'organisation. Il est essentiel de déterminer les sites de l'organisation, les départements, les services, ainsi que les infrastructures techniques impliquées dans l'exercice.

Identifier également les lieux physiques où l'exercice se déroulera est une composante clé du périmètre. Ces sites offrent un cadre réaliste pour tester les réactions et la coordination des équipes face à des incidents simulés.

Il est important de préciser les restrictions et limitations en identifiant les départements, sites et systèmes exclus de l'exercice, tout en expliquant les raisons de leur exclusion.

Activité 7. Constituer une équipe de préparation

La constitution d'une équipe de préparation est une étape essentielle pour assurer le succès d'un exercice de gestion de crise. Cette équipe est responsable de planifier, coordonner et superviser l'ensemble des activités liées à l'exercice.

La première étape consiste à former une équipe de spécialistes qui apporteront leur expertise respective pour établir un scénario réaliste et pertinent. Les membres de l'équipe de préparation, en raison de leur implication directe dans la conception et la planification de l'exercice, ne pourront pas participer activement à l'exercice lui-même.

Leur rôle est d'assurer que tous les aspects de l'exercice sont couverts et que les ressources nécessaires sont disponibles et correctement utilisées.

Activité 8. Déterminer les participants et les observateurs

Sélectionner les participants et les observateurs est une étape essentielle pour la réussite de l'exercice de gestion de crise.

Cette sélection doit être réalisée de manière stratégique et réfléchie afin de garantir que tous les aspects critiques de la gestion de crise sont couverts de manière efficace et réaliste.

- **Participants :** Ils sont sélectionnés en fonction du type d'exercice, du périmètre et des objectifs à atteindre. Par exemple, pour un exercice de gestion de crise, les participants immergés dans la simulation seront les membres titulaires de la cellule de crise décisionnelle. Leur rôle est de gérer la crise en utilisant toute la documentation mise à leur disposition et de collaborer efficacement pour résoudre les problèmes qui se présentent. Ils doivent appliquer les procédures de gestion de crise, communiquer clairement et prendre des décisions cruciales pour gérer la situation tout en faisant face aux divers défis simulés par l'exercice.
- **Observateurs :** Comme leur nom l'indique, ils sont là pour observer l'exercice et n'interviennent pas pendant son déroulement. Leur rôle est d'analyser le déroulement de l'exercice, de noter les interactions entre les participants et de fournir des retours constructifs qui aideront à identifier les points forts ainsi que les domaines nécessitant des améliorations. Inclure des membres de l'équipe de préparation parmi les observateurs peut être particulièrement bénéfique, car leur connaissance détaillée du scénario et des objectifs de l'exercice leur permet de fournir des observations particulièrement pertinentes.

Activité 9. Prévoir un budget et la logistique de l’exercice

Prévoir un budget et organiser la logistique sont des étapes cruciales pour la réussite de tout exercice de gestion de crise.

Ces éléments garantissent que toutes les ressources nécessaires sont disponibles et que l’exercice se déroule sans encombre. La première étape consiste à établir un budget couvrant tous les aspects de l’exercice. Cela inclut :

- **Location des espaces :** Si l’exercice nécessite des espaces spécifiques, prévoir les coûts de location des salles de réunion ou des centres de formation.
- **Déplacements et hébergement :** Si des participants doivent se déplacer, inclure les coûts de transport, d’hébergement et de repas.
- **Restauration :** Organiser des services de restauration pour les participants, surtout si l’exercice dure une journée entière ou plus.
- **Personnel d’astreinte et consultants externes :** Si du personnel d’astreinte, des fournisseurs avec lesquels vous travaillez, des consultants ou experts externes sont impliqués dans l’exercice, inclure leurs honoraires.

Une fois le budget établi, la planification logistique doit être organisée avec soin pour assurer le bon déroulement de l'exercice :

- Désignez une personne responsable de la logistique qui sera le point de contact pour toute question ou problème éventuel.
- Réservez toutes les salles nécessaires en s'assurant que chaque cellule de crise dispose de son propre espace de travail équipé des moyens de communication adéquats.
- Testez tous les équipements avant l'exercice pour garantir qu'ils fonctionnent correctement le jour J, incluant les ordinateurs, les systèmes de communication et tout autre matériel technique.
- Coordonnez les déplacements des participants, prévoyez des solutions d'hébergement si nécessaire et organisez les transferts entre les différents sites de l'exercice.
- Planifiez les repas et les pauses café pour maintenir l’énergie et la concentration des participants tout au long de l’exercice.
- Assurez une signalisation claire des lieux de l’exercice pour que les participants trouvent facilement leur chemin et respectent les consignes de sécurité.

Activité 10. Réaliser un rétro-planning

Pour garantir la réussite de l’exercice de gestion de crise, il est essentiel de réaliser un rétro-planning détaillé.

Cette planification permet de structurer et de coordonner toutes les étapes préparatoires afin que chaque tâche soit effectuée en temps voulu, assurant ainsi une préparation optimale. Une coordination efficace est cruciale pour que toutes les parties prenantes soient informées des aspects logistiques.

Créez un calendrier précis des préparatifs et des vérifications à effectuer avant l’exercice. En détaillant chaque tâche avec des échéances spécifiques, vous vous assurez que rien n'est oublié et que chaque aspect de l'exercice est prêt à temps.

En intégrant ces éléments dans votre rétro-planning, vous établissez une base solide pour la préparation de l’exercice de gestion de crise.

Étape 3 : Définir le déroulement de l'exercice

Planifier le déroulement de l'exercice de gestion de crise implique de créer un scénario réaliste et pertinent ainsi que de produire les outils nécessaires pour sa mise en œuvre. Cette étape est essentielle pour garantir que l'exercice se déroule de manière fluide et structurée, offrant aux participants une expérience immersive et formatrice. Un scénario bien conçu et des outils adéquats permettent aux participants de se plonger pleinement dans la simulation, de réagir de manière appropriée aux événements et de tirer des leçons précieuses pour la gestion des crises réelles.

Activité 11. Rédiger le scénario

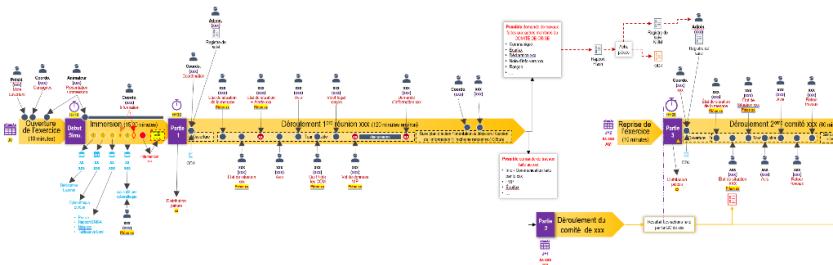
Le scénario est la colonne vertébrale de l'exercice de gestion de crise. Il doit être conçu de manière à refléter des situations réalistes et des défis plausibles que l'organisation pourrait rencontrer.

- **Identifier les menaces :** fondé sur une analyse des risques, le scénario doit inclure des événements qui pourraient réellement se produire. Cela signifie examiner les vulnérabilités de l'organisation, les tendances actuelles des menaces et les incidents passés. Par exemple, une entreprise technologique pourrait simuler une cyberattaque tandis qu'une entreprise de transport pourrait simuler une catastrophe naturelle affectant ses opérations.
- **Incorporer des détails spécifiques :** le scénario doit être riche en détails pour rendre la simulation aussi réaliste que possible. Cela inclut la nature de la crise, les déclencheurs, les impacts attendus et les réponses initiales. Les détails peuvent inclure des incidents spécifiques comme une panne de système, des communications interrompues ou des demandes de rançon qui forcent les participants à réagir de manière appropriée.
- **Prévoir des évolutions dynamiques :** le scénario doit être suffisamment flexible pour évoluer en fonction des actions des participants, permettant ainsi de tester leur capacité à s'adapter à des situations changeantes. Par exemple, si les participants réussissent à contenir une menace initiale, le scénario pourrait introduire une nouvelle complication comme une attaque secondaire ou une fuite de données.
- **Impliquer les experts de contenu :** les experts de contenu, membres de l'équipe de préparation, jouent un rôle crucial dans la réalisation du scénario. Leur expertise spécifique permet d'enrichir le scénario avec des détails techniques et contextuels réalistes. Ils apportent des connaissances précieuses sur les aspects opérationnels, techniques et stratégiques de l'organisation, garantissant que le scénario est pertinent et fidèle aux réalités de l'entreprise.

Activité 12. Produire le chronogramme

Un chronogramme détaillé est essentiel pour structurer et coordonner efficacement l'exercice de gestion de crise. Il offre une vision d'ensemble des moments clés, des actions à entreprendre et des points de contrôle, garantissant ainsi que l'exercice se déroule de manière fluide et reste sur la bonne voie.

- **Élaborer un emploi du temps précis :** le chronogramme doit indiquer les moments clés de l'exercice, les actions à entreprendre ainsi que les actions attendues. Il a pour objectif de :
  - Maintenir le rythme en définissant clairement chaque étape et de s'assurer que l'exercice progresse de manière ordonnée et structurée.
  - Faciliter l'introduction de nouveaux éléments en précisant les moments où l'équipe d'animation peut introduire de nouvelles informations ou défis, maintenant ainsi la dynamique de l'exercice.
- **Inclure les éléments clés :** le chronogramme doit inclure plusieurs éléments essentiels pour une gestion efficace de l'exercice :
  - Définissez le moment précis où la crise fictive commence ainsi que les premiers signaux d'alerte.
  - Identifiez les points où les participants doivent prendre des décisions. Ces moments doivent être clairement indiqués pour s'assurer que les participants comprennent l'importance de leurs actions à ces étapes.
  - Prévoyez des moments spécifiques pour évaluer la progression de l'exercice et ajustée si nécessaire. Ces points permettent de vérifier que les objectifs sont atteints et que l'exercice reste aligné sur le scénario prévu.



Activité 13. Déterminer les rôles à simuler

Déterminer les rôles à simuler est une étape cruciale dans la planification de l'exercice de gestion de crise.

Cette phase consiste à identifier et définir les différents personnages et rôles fictifs nécessaires pour recréer une situation de crise réaliste et complète.

Un exercice bien structuré doit inclure une diversité de rôles représentant toutes les fonctions critiques de l'organisation afin de tester et améliorer la réactivité et la coordination de l'équipe en situation de crise.

Parmi les membres de l'équipe de préparation, certaines personnes doivent jouer des rôles d'intervenants externes fictifs pour ajouter du réalisme à l'exercice. Ces rôles fictifs peuvent inclure des journalistes, des représentants gouvernementaux ou des clients mécontents qui interagissent avec l'organisation pour tester sa capacité de réponse à la pression extérieure.

Voici quelques exemples : Des membres de l'équipe peuvent jouer le rôle de journalistes posant des questions incessantes et parfois difficiles, testant ainsi la capacité des responsables de la communication à gérer la pression médiatique.

D'autres peuvent simuler des interactions avec des représentants des autorités locales ou nationales, ajoutant une couche de complexité à la gestion de la crise. Ils peuvent également jouer le rôle de clients mécontents, obligeant les participants à gérer les communications externes et à maintenir les relations professionnelles.

Activité 14. Préparer les différentes pièces

Préparer des intrants pour rythmer l'exercice est une étape essentielle pour garantir la crédibilité de la simulation.

Cela implique de développer des supports visuels et des documents nécessaires qui permettront aux participants de naviguer efficacement à travers les différentes phases de l'exercice. Ces supports doivent être réalistes et alignés avec le scénario pour renforcer l'immersion et la pertinence de l'exercice. Voici des exemples de pièces qui peuvent être produites :

- Faux rapports d'incidents : détaillez des problèmes spécifiques qui surviennent pendant la crise. Ces rapports doivent inclure des analyses de la cause, des impacts prévus et des recommandations pour les actions à entreprendre.
- Coupures de presse fictives : simulez la communication externe.
- Alertes et notifications simulées : informez les participants des développements en temps réel. Cela peut inclure des courriels simulant des communications internes, des messages d'urgence ou des mises à jour de la situation.
- Fiches techniques et autres documents spécialisés : nécessaires pour gérer les aspects techniques de la crise.

Il est essentiel que tous les supports préparés soient intégrés de manière cohérente dans le scénario de l'exercice. Chaque document doit correspondre à une étape spécifique du chronogramme et être utilisé de manière à renforcer les objectifs pédagogiques de l'exercice.

Activité 15. Préparer le support de l'exercice

Il est essentiel de créer un support complet et cohérent qui orientera les participants tout au long de l'exercice.

Ce support doit être informatif, visuellement attrayant et facile à comprendre afin de garantir une immersion totale et une participation efficace.

Étape 4 : Effectuer une répétition de l'exercice

Effectuer une répétition de l'exercice est une étape indispensable dans la préparation d'un exercice de gestion de crise.

Cette répétition permet de tester et d'ajuster le scénario, d'identifier les éventuels problèmes et de s'assurer que tous les détails sont prêts avant l'exercice réel.

En simulant l'exercice dans des conditions aussi proches que possible de la réalité, les organisateurs peuvent anticiper les défis, affiner les plans et garantir que tous les participants comprennent leurs rôles et responsabilités.

Cette étape aide à améliorer l'efficacité globale de l'exercice.

Activité 16. Répéter le scénario de l'exercice avec l'équipe de préparation

En répétant le scénario de l'exercice avec l'équipe de préparation, vous pouvez anticiper et résoudre les problèmes potentiels, améliorer la qualité du scénario et renforcer la confiance des participants.

Cette étape est essentielle pour garantir le succès de l'exercice de gestion de crise et pour préparer efficacement l'organisation à faire face à de véritables situations de crise.

Voici comment aborder cette activité :

- Planifiez la répétition et préparez tous les matériels et supports requis. Assurez-vous que la répétition soit aussi réaliste que possible pour identifier les défis potentiels.
- Exécutez le scénario avec l'équipe de préparation en jouant les différents rôles. Cette simulation permet de tester la fluidité du scénario et d'identifier les problèmes.
- Tenez une session de compte rendue après la répétition pour recueillir les rétroactions, analyser les écarts et ajuster le scénario en conséquence. Modifiez les éléments problématiques pour améliorer la fluidité et la pertinence de l'exercice.
- Mettez à jour les supports de simulation.

PHASE 2 – EXÉCUTION DE L'EXERCICE

La phase d'exécution est le moment de vérité où la préparation prend vie. C'est ici que les scénarios se déploient, que les participants mettent en pratique leurs compétences et que la résilience de l'organisation est mise à l'épreuve. Une exécution maîtrisée est essentielle pour tirer pleinement parti de l'exercice et obtenir des résultats significatifs.

Cette phase inclut plusieurs étapes : la présentation des consignes, la mise en situation des participants, le suivi du déroulement du scénario et la gestion des réactions imprévues. Chaque action et réaction est observée et analysée pour fournir des retours constructifs. Une gestion efficace de l'exercice garantit non seulement une expérience immersive et réaliste, mais aussi des leçons précieuses pour améliorer les capacités de réponse de l'organisation.

Dans cette section, nous explorerons chaque étape de l'exécution en fournissant des conseils et des recommandations pour maximiser l'impact de l'exercice et assurer une gestion sans faille des événements simulés.

Étape 5 : Animer l'exercice

L'animation d'un exercice de gestion de crise est une étape déterminante qui permet de mettre en pratique les connaissances théoriques et les protocoles établis. En simulant une situation de crise réaliste, les participants peuvent tester leur capacité à réagir de manière adéquate, à communiquer efficacement et à collaborer sous pression.

Cette phase de l'exercice est structurée en plusieurs activités clés qui assurent une gestion fluide et productive de la simulation tout en offrant des opportunités d'apprentissage et d'amélioration continue.

Activité 17. Présenter les consignes du déroulement de l'exercice

La première étape de l'animation consiste à expliquer les règles de l'exercice aux participants.

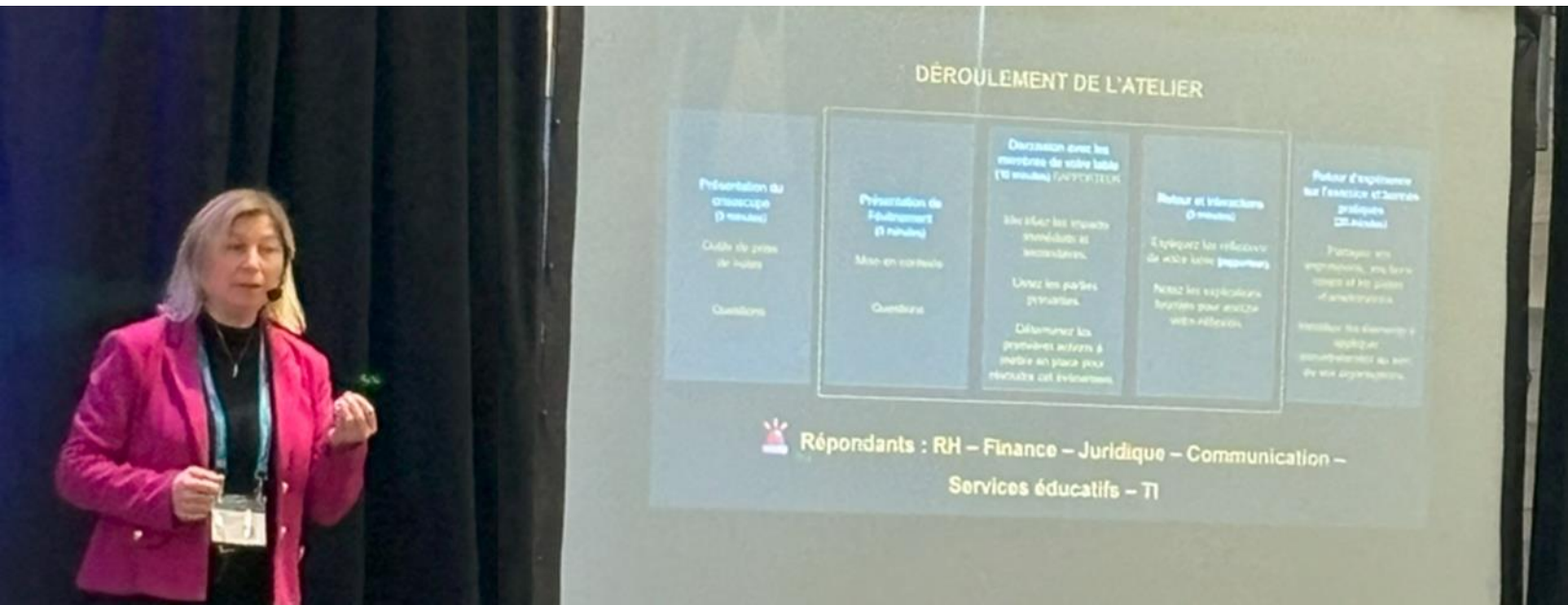
Cette phase est essentielle pour garantir que tous comprennent les attentes et les consignes à suivre.

Une présentation claire et détaillée des consignes assure que chacun est bien préparé, connaît ses rôles et responsabilités et est prêt à collaborer efficacement pour atteindre les objectifs de l'exercice.

En définissant des lignes directrices claires pour le déroulement de l'exercice, on peut maintenir une structure et un ordre tout au long de la simulation.

Voici quelques exemples de consignes :

- Utilisez uniquement la documentation mise à votre disposition.
- Ayez une communication claire et concise. Des messages précis et directs facilitent la compréhension rapide et la prise de décision efficace.
- Plusieurs événements seront simulés dans un court délai et l'exercice se déroulera à huis clos.
- Soulignez l'importance d'une participation active tout au long de l'exercice. Chaque membre doit s'impliquer pleinement dans son rôle pour garantir le réalisme et l'efficacité de l'exercice.
- Invitez à noter observations et impressions. Ces notes seront précieuses pour le compte rendu post-exercice et pour l'amélioration des futurs exercices.



Activité 18. Mettre les membres de la cellule de crise en situation

Mettre les membres de la cellule de crise en situation consiste à les immerger dans des conditions de crise simulées afin de tester leurs réactions, leur coordination et leur capacité à gérer des situations d'urgence. Cette activité est essentielle pour évaluer et renforcer la préparation de l'équipe à faire face à une crise réelle.

L'objectif est de recréer un environnement aussi réaliste que possible où les participants peuvent immédiatement se plonger dans le scénario et réagir comme ils le feraient en situation réelle.

Pour atteindre cet objectif, il est essentiel d'installer le décor de la crise de manière à créer une atmosphère immersive et crédible. Voici comment procéder :

- Commencez par décrire la situation initiale de la crise. Expliquez les circonstances entourant l'événement, les enjeux et les défis spécifiques que l'équipe devra affronter. Ce contexte aide les participants à comprendre l'ampleur de la crise et leur rôle dans sa gestion.
- Utilisez des enregistrements audios pour simuler des sons de sirènes, d'alertes, de foules en panique ou de perturbations environnementales comme des tempêtes ou des explosions. Ces éléments sonores contribuent à créer une tension réaliste.
- Ajustez l'éclairage de la salle pour refléter des conditions de crise comme des pannes d'électricité ou des situations de faible visibilité. Les lumières tamisées ou clignotantes peuvent simuler l'ambiance d'une salle de commande en crise.
- Placez des écrans autour de la salle affichant des alertes en temps réel, des mises à jour de la situation et des informations cruciales. Utilisez des graphismes et des animations pour représenter la propagation de la crise, les mouvements de foule ou les dégâts subis.
- Utilisez des décors ou des effets spéciaux pour simuler des dommages physiques tels que des bâtiments endommagés, des routes bloquées ou des systèmes informatiques en panne. Ces éléments visuels aident à rendre la crise plus tangible et à solliciter des réponses adaptées.

Activité 19. Suivre le déroulement du chronogramme

Suivre le déroulement du chronogramme est essentiel dans l'animation d'un exercice de gestion de crise. Cette activité consiste à s'assurer que chaque étape du scénario se déroule comme prévu.

Une gestion rigoureuse du chronogramme permet de maintenir la structure de l'exercice, d'identifier rapidement les déviations et de prendre des mesures correctives si nécessaire.

En respectant le rythme prédéfini, toutes les étapes sont couvertes sans déviation significative, assurant ainsi la cohérence de l'exercice.

La détection rapide des écarts permet d'intervenir immédiatement pour corriger la trajectoire de l'exercice, prévenant tout problème potentiel avant qu'il ne devienne critique.

Un rythme structuré et prévisible garde les participants engagés et assure une participation active et efficace. Lorsque les participants savent à quoi s'attendre et peuvent suivre le déroulement de l'exercice sans surprises majeures, ils restent concentrés et motivés.

Cet engagement continu est crucial pour le succès de l'exercice, car il garantit que tous les participants contribuent activement et de manière productive.

Pour garantir le bon déroulement de l'exercice, il est essentiel de surveiller chaque étape du chronogramme et d'intervenir rapidement en cas de déviation significative. Cela permet de remettre l'exercice sur la bonne voie et d'assurer une meilleure gestion de crise.

Activité 20. Savoir répondre aux réactions imprévues

Répondre de manière flexible aux actions imprévues est une compétence essentielle dans la gestion de crise.

Malgré la réalisation d'un chronogramme détaillé, il y aura toujours des imprévus à gérer pendant un exercice. L'animateur doit s'adapter à ces imprévus pour maintenir la fluidité et l'efficacité de l'exercice.

Cette activité consiste à adapter rapidement et efficacement les réponses aux situations non prévues qui surgissent pendant l'exercice.

La capacité à gérer les imprévus de façon dynamique permet de maintenir le déroulement de l'exercice tout en offrant des opportunités d'apprentissage précieuses.

Voici comment aborder cette activité :

- Préparez des scénarios alternatifs pour différentes éventualités. Avoir des plans B permet d'adapter rapidement le scénario en fonction des actions des participants.
- Encouragez l'équipe à rester flexible et ouverte à l'imprévu. La préparation mentale à gérer les surprises améliore la réactivité et la résilience.
- Surveillez en temps réel les actions des participants et les développements de la crise simulée pour identifier rapidement les déviations du plan initial.
- Notez les imprévus et les réactions pour une analyse post-exercice. La documentation aide à comprendre les dynamiques de l'équipe et les points à améliorer.
- Prenez des décisions rapides pour ajuster le scénario en fonction des nouvelles informations. Une intervention rapide est cruciale pour maintenir la fluidité de l'exercice.
- Modifiez le scénario en temps réel pour intégrer les nouvelles actions ou événements. Assurez-vous que ces ajustements restent réalistes et pertinents pour les objectifs de l'exercice.

Activité 21. Remercier les participants

Exprimer sa gratitude envers les participants est une étape essentielle dans l'animation d'un exercice de gestion de crise.

Cette activité permet de reconnaître l'engagement et les efforts des participants, de renforcer leur motivation et de susciter l'envie de participer à de futurs exercices.

En prenant le temps de remercier les participants de manière sincère et structurée, vous contribuez à créer un environnement positif et motivant, propice à la répétition des exercices et à une préparation efficace face aux crises futures. Cela aide également à développer une culture de résilience au sein de l'organisation. Voici quelques gains de ces remerciements :

- **Renforcement de la motivation et de la cohésion d'équipe :** remerciez les participants contribue à renforcer leur motivation et leur engagement pour les futurs exercices et activités, tout en favorisant la cohésion et l'esprit d'équipe par un sentiment de reconnaissance collective.
- **Résumé des performances globales :** donnez un bref résumé des performances globales, en mettant en avant les aspects positifs et les succès de l'exercice. Cela met en lumière les efforts collectifs et individuels.
- **Culture de résilience :** infusez, une culture de résilience où les efforts et les contributions sont régulièrement célébrés et appréciés, encourageant une préparation continue et une capacité accrue à faire face aux crises futures.

Activité 22. Organiser un retour d'expérience à « chaud »

Organiser un retour d'expérience (RETEX) à « chaud » consiste à tenir une séance de compte rendue immédiatement après l'exercice pour recueillir les premières impressions et les retours des participants.

Cette discussion aide à capter les réactions et sentiments des participants avant que les détails ne soient oubliés et d'identifier les points forts et pistes d'améliorations. Voici comment aborder cette activité :

Encouragez les participants à partager leurs expériences et observations sans filtre pour obtenir une rétroaction honnête et directe. Cela permet de détecter des problèmes ou des succès grâce aux retours spontanés, de collecter des idées et suggestions pour améliorer les futurs exercices et d'identifier des actions immédiates pour corriger les faiblesses ou renforcer les plans qui permettent de gérer une crise.

Le RETEX se fait sous la forme d'un tour de table. Donnez à chaque participant l'occasion de s'exprimer en répondant à des questions ouvertes telles que : « Quelles sont vos premières impressions sur l'exercice ? », « Quels ont été les moments les plus marquants pour vous ? », « Qu'auriez-vous fait différemment ? » et « Quelles sont les pistes d'améliorations ? »

Notez toutes les observations pour faciliter leur analyse et le suivi des actions correctives. Ces observations seront également utiles pour la rédaction d'un bilan.

PHASE 3 – APPRENTISSAGE ET AMÉLIORATION CONTINUE

La phase d'apprentissage et d'amélioration continue est cruciale pour transformer l'expérience d'un exercice de gestion de crise en une véritable opportunité de progression. Après l'exercice, l'analyse minutieuse des performances et des réactions permet de tirer des leçons précieuses et de renforcer les plans de gestion de crise.

Cette phase comprend plusieurs étapes essentielles : organiser des retours d'expérience à froid, produire un bilan détaillé de l'exercice et traiter les pistes d'améliorations. Elle implique également l'actualisation des documents de gestion de crise pour intégrer les enseignements tirés. En capitalisant sur ces leçons, l'organisation améliore sa résilience et sa préparation face aux crises futures.

Dans cette section, nous présenterons chaque étape de la phase d'apprentissage et d'amélioration continue avec des conseils pour que chaque exercice améliore la gestion de crise de l'organisation.

Étape 6 : Capitaliser sur les leçons apprises

Analyser les performances et les enseignements tirés des exercices de gestion de crise est une étape cruciale pour renforcer ces procédures et mieux préparer l'organisation aux défis futurs. Cette analyse permet non seulement d'identifier les points forts et les faiblesses, mais aussi de transformer les leçons apprises en actions concrètes et constructives.

Activité 23. Planifier un retour d'expérience à « froid »

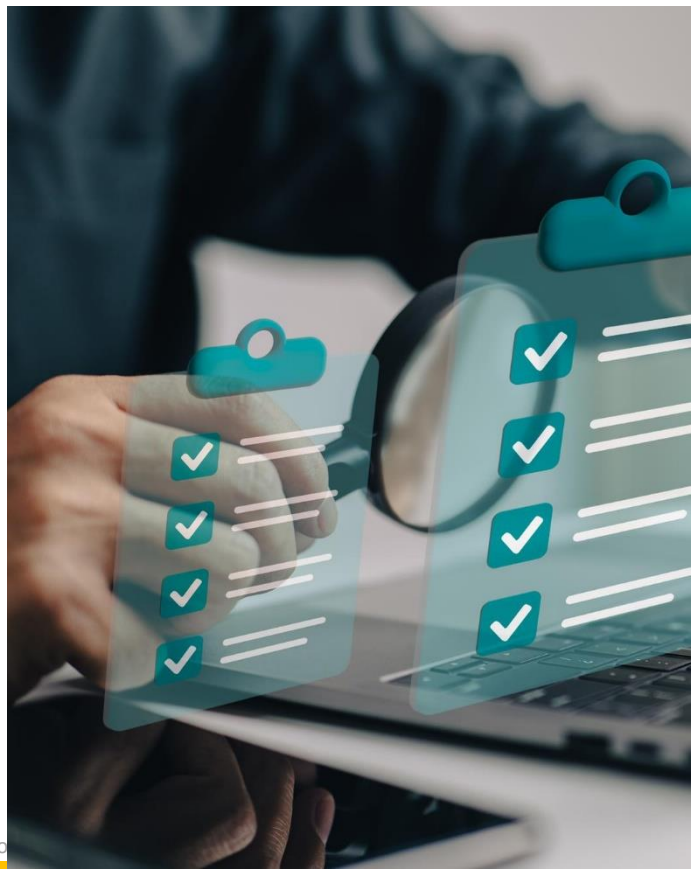
Quelques jours après votre exercice de gestion de crise, il est conseillé d'organiser un RETEX à "froid". Ce dernier complète le RETEX à "chaud" effectué immédiatement après l'exercice, qui capte les premières impressions et réactions des participants. Cependant, en raison de l'intensité du moment, ces premières impressions peuvent être incomplètes.

Le RETEX à "froid", réalisé après un certain délai, offre aux participants l'occasion de prendre du recul et de réfléchir de manière plus critique et objective aux événements, facilitant ainsi une analyse plus détaillée et précise des performances de l'exercice.

Pour structurer ce processus, le responsable de l'exercice envoie un questionnaire détaillé à tous les participants. Ce questionnaire devrait couvrir tous les aspects de l'exercice, y compris les points forts, les faiblesses et les suggestions d'amélioration. Ainsi, les participants ont l'opportunité de réfléchir individuellement et de consigner leurs observations de manière organisée.

Ce temps de recul est essentiel. Il permet aux participants de digérer les événements et de développer une perspective plus critique et objective, enrichissant l'analyse globale de l'exercice.

Les informations recueillies lors de ces RETEX serviront de base pour produire un bilan complet qui guidera les améliorations futures des procédures de gestion de crise.



Activité 24. Produire le bilan de l'exercice

La rédaction d'un bilan après un exercice de gestion de crise est essentielle pour exploiter pleinement les enseignements tirés.

Ce rapport doit condenser efficacement les observations, les résultats et les leçons apprises, offrant ainsi une analyse complète et réfléchie des performances observées durant l'exercice.

Plus qu'une simple formalité, ce rapport est un outil stratégique crucial pour l'amélioration continue de la gestion de crise.

Il met en avant les succès et identifie les axes d'amélioration, jouant un rôle déterminant dans la préparation des organisations. Grâce à lui, les organisations peuvent affiner leurs stratégies pour gérer plus efficacement les crises futures. Voici ce que doit contenir le bilan :

- **Introduction :** contextualise l'exercice de gestion de crise en détaillant les objectifs, la date, le lieu, les participants et la nature des scénarios simulés. Elle vise à établir une compréhension claire des enjeux et attentes de l'exercice pour les lecteurs.
- **Points forts :** révèlent l'efficacité des stratégies et des compétences déployées face à des situations d'urgence simulées. Un aspect valorisé est la rapidité et la précision des réactions des équipes, témoignant de leur préparation et de leur capacité à suivre les procédures établies sous pression. Une communication fluide et efficace entre les différents groupes est également cruciale, car elle assure une coordination sans faille et une prise de décision rapide et informée. L'utilisation optimale des outils et technologies disponibles, adaptées aux besoins spécifiques de la crise simulée, démontre l'aptitude des participants à exploiter les ressources à leur disposition pour gérer efficacement l'urgence. De plus, la capacité d'adaptation des équipes face à des scénarios imprévus ou des complications soudaines souligne leur flexibilité et leur créativité, des qualités essentielles pour la résolution de crises. Ces points forts, lorsqu'ils sont identifiés et renforcés, contribuent à bâtir une organisation résiliente et prête à affronter des défis complexes.
- **Axes d'amélioration :** joue un rôle crucial dans le renforcement continu des capacités de gestion de crise de l'organisation. Cette section est méthodiquement structurée. Elle commence par définir les solutions spécifiques à mettre en œuvre pour adresser les problèmes identifiés lors de l'exercice. Chaque solution est assortie d'une priorité, permettant de trier les actions selon leur urgence et leur impact potentiel. Pour chaque action proposée, un responsable est désigné, garantissant ainsi l'attribution claire des tâches et la responsabilisation des équipes. En somme, les pistes d'amélioration ne se contentent pas de corriger les problèmes ; elles servent de feuille de route pour l'évolution systématique de l'organisation dans sa gestion de crises, assurant ainsi que chaque exercice contribue de manière constructive à renforcer les capacités globales de l'organisation.

Activité 25. Présenter les résultats

Partager les conclusions du rapport de résultat de la simulation de gestion de crise avec toutes les parties prenantes, y compris la direction et les équipes opérationnelles, est une pratique cruciale pour maximiser l'impact des enseignements tirés.

Une communication efficace des résultats permet non seulement d'informer chaque niveau de l'organisation des performances actuelles et des améliorations nécessaires, mais elle sert aussi à renforcer la compréhension commune des objectifs de gestion de crise et des méthodes pour y parvenir.

Pour être efficace, cette présentation doit être claire et concise, mettant en évidence les principaux résultats, les points forts à maintenir et les faiblesses à adresser. L'utilisation de graphiques, de tableaux et de résumés peut faciliter la compréhension et l'engagement des parties prenantes en rendant l'information plus accessible et plus rapide à digérer. Par exemple, illustrer les résultats avec des comparaisons avant et après l'exercice peut clairement montrer où des progrès ont été faits et où des efforts supplémentaires sont nécessaires.

Étape 7 : Améliorer la gestion de crise

Améliorer la gestion de crise ne consiste pas seulement à réagir adéquatement en temps de crise, mais également à anticiper les défis et à se préparer activement à y faire face. Pour cela, il est essentiel de mettre en œuvre les actions correctives identifiées lors des exercices et des situations réelles et d'actualiser continuellement les plans existants.

Cela permet de renforcer la résilience de l'organisation, d'assurer une préparation robuste et de minimiser les impacts négatifs des futurs événements disruptifs. En investissant dans l'amélioration continue de la gestion de crise, les organisations peuvent non seulement protéger leurs ressources, mais aussi tirer avantage des opportunités qui émergent dans des situations de pression et de changement.

Activité 26. Traiter les pistes d'amélioration

Pour aborder efficacement les pistes d'améliorations identifiées lors d'un exercice de gestion de crise, un plan d'action détaillé et structuré est essentiel.

Ce plan doit intégrer plusieurs étapes clés pour garantir que les améliorations nécessaires ne sont pas seulement mises en œuvre, mais qu'elles entraînent également des avancées tangibles au sein de l'organisation. Voici comment un tel plan peut être élaboré pour optimiser les résultats :

- Assignez clairement la responsabilité de la mise en œuvre de chaque action à des individus ou des équipes spécifiques. Cette assignation favorise la responsabilisation et garantit un engagement fort dans le processus d'amélioration.
- Créez un calendrier détaillé pour l'implémentation des améliorations, définissant des échéances pour les étapes clés et organisant des revues périodiques pour évaluer les progrès.
- Mettez en place un système de suivi régulier pour vérifier l'avancement des actions d'amélioration et évaluer leur efficacité. Adaptez le plan selon les résultats obtenus et les rétroactions reçues.

Activité 27. Actualiser la documentation de gestion de crise

L'actualisation de la documentation de gestion de crise est une démarche essentielle qui permet d'assurer que l'organisation est prête et résiliente face aux défis futurs.

Cette pratique consiste à réviser et à mettre à jour régulièrement les plans de gestion de crise et les documents de référence en intégrant les améliorations issues d'un exercice de gestion de crise. Voici comment cette mise à jour continue peut-être réalisée de manière efficace :

- Actualisez vos documents de gestion de crise en intégrant les connaissances et les enseignements tirés des dernières interventions et des exercices de simulation récents. L'objectif est d'optimiser les plans existants pour qu'ils soient plus robustes et adaptés aux défis émergents, assurant ainsi une réponse plus efficace lors de futures crises.
- Envoyez les documents mis à jour à toutes les parties prenantes.
- Organisez des sessions d'information pour vous assurer que chaque membre de l'équipe comprend les ajustements.

La réalisation d'un exercice de gestion de crise bien préparé et exécuté est un investissement précieux dans la résilience organisationnelle. Ce dossier vous a proposé une feuille de route détaillée, guidant chaque étape depuis la préparation jusqu'à l'apprentissage et l'amélioration continue.

En suivant ce guide structuré, vous pourrez identifier et renforcer les compétences essentielles, améliorer la coordination interne, et affiner les plans de gestion de crise de votre organisation.

Chaque phase, de la conception initiale à l'analyse post-exercice, contribue à créer un environnement où la réactivité et l'efficacité en situation de crise sont maximisées. Les retours d'expérience, tant à chaud qu'à froid, permettent de capitaliser sur les leçons apprises, transformant les défis rencontrés en opportunités d'amélioration continue.

Vous l'aurez compris en lisant ce dossier, un exercice de gestion de crise ne se limite pas à une simulation ponctuelle; il s'agit d'un processus dynamique et itératif qui renforce la capacité de votre organisation à anticiper, répondre et s'adapter aux crises futures.

Il va de soi qu'en intégrant ces pratiques dans votre culture organisationnelle, vous favoriserez une attitude proactive et résiliente face aux imprévus.

Nous espérons que ce guide vous sera utile pour concevoir et mener à bien vos exercices de gestion de crise, et qu'il contribuera à la création d'une organisation mieux préparée et plus résistante aux aléas.

Continuer à apprendre et à s'adapter est essentiel pour rester efficace et capable de protéger vos ressources, vos employés et vos intérêts dans un monde en constante évolution.

Karine Maréchal-Richard

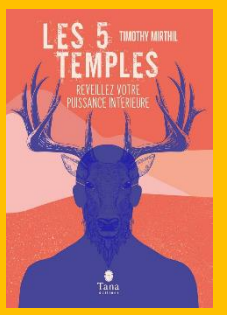
CRISE & RÉSILIENCE
L'ART DE SURVIVRE AUX CRISES

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

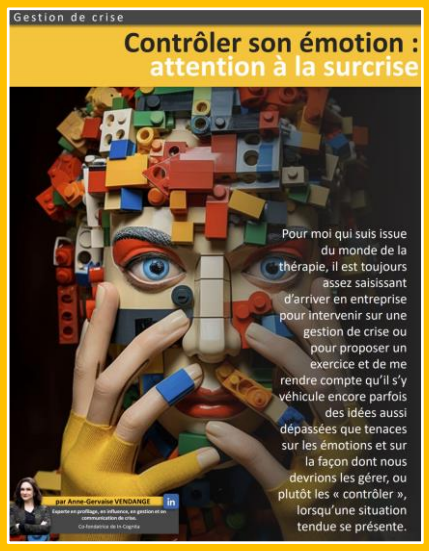
Timothy Mirthil-de Segonzac

Journaliste et auteur spécialiste de la gestion du stress et expert pour l'Agence The Trusted Agency.



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

Avez-vous lu ces articles ?



criseetresilience-magazine.com

Préparer les scénarios de crise grâce à la visualisation.

Facile, ludique et infinie, la visualisation est l'un des grands secrets de la performance. Cette technique utilise l'imagination concrète afin de concrétiser ses objectifs.

Elle est pratiquée par tous les athlètes de haut niveau, les pilotes, les skieurs, les parachutistes ou pratiquants de sports de combat ?

Les unités d'élite l'utilisent également.

Alors pourquoi pas vous ?

Visualisation émotionnelle pour la préparation

Prenez un moment pour vous connecter émotionnellement avec les scénarios de crise. Visualisez-vous ressentir les émotions que ces situations pourraient susciter chez vous : le stress, l'anxiété, mais aussi la détermination et la confiance en votre équipe et en la mission. Pensez-vous maitre dans l'action.

Visualisation des étapes du processus

Visualisez-vous en équipe en train de suivre les étapes du processus de résolution préalablement définies. Imaginez-vous en train de mettre en œuvre ces étapes de manière fluide et efficace, en surmontant les obstacles avec confiance et détermination.

Visualisation de la communication en équipe

Vous allez forcément devoir gérer des blocages et des mésententes au sein de votre équipe.

Ces erreurs de communication inter-individuelles sont la principale l'origine d'un échec de la mission.

Alors incluez votre équipe dans cette visualisation.

Ensemble, fermez les yeux et imaginez la manière dont vous allez communiquer pendant la crise. Visualisez-vous en train d'identifier rapidement les blocages dans la communication et les conflits potentiels, et en train de les résoudre de manière proactive pour maintenir une collaboration efficace et une prise de décision rapide.

Ne sous estimez pas ce travail en préparation.

La visualisation permet de renforcer la préparation mentale et opérationnelle des individus et des équipes face à des situations de haute intensité, favorisant ainsi des réponses efficaces et coordonnées.

Passe à l'action!

ABONNEZ-VOUS Gratuitement

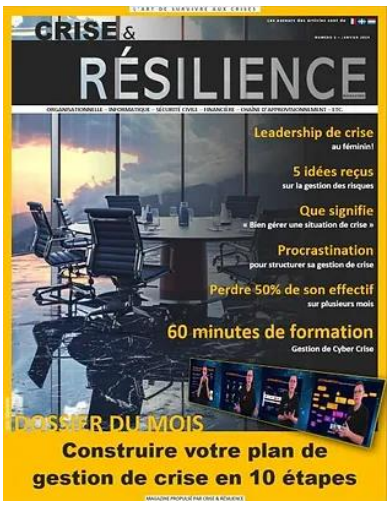
TRIMESTRIEL – JANVIER – AVRIL – JUILLET – OCTOBRE

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

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

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

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



Abonnez-vous gratuitement sur 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**. 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 !

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.

La continuité d'activité, une démarche multidisciplinaire

« Les plans ont peu d'importance, mais la planification est essentielle. »
Winston Churchill

La démarche de continuité d'activité ne doit pas se limiter à sa seule composante : le plan de continuité des affaires (PCA).
Le PCA est un des livrables indispensables, mais seul, il n'est qu'un papier.

par Bastien Monate
Chef de la mission continuité d'activité
En charge de la démarche de continuité d'activité pour le ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique

Il faut penser la continuité d'activité comme un écosystème à mobiliser et à rassembler autour de valeurs communes dans le but de résister collectivement le mieux possible aux tempêtes que nous allons rencontrer.

1. La continuité d'activité est indissociable de la gestion de crises et n'est possible qu'avec des acteurs préidentifiés formés et entraînés

La continuité d'activité ne peut être portée par un seul individu, qu'il soit cadre ou dirigeant. Elle doit être l'affaire de tous pour maximiser les chances de réussite des solutions de reprise d'activité intégrées dans les PCA. Ainsi, nous sommes bien dans une logique d'animation d'une communauté de continuité d'activité qui doit se connaître, apprendre à travailler ensemble et, dans la mesure du possible, être pluridisciplinaire.

Au sein de l'État français, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) organise chaque année deux exercices majeurs interministériels, dans l'optique de tester la mise à jour de plans gouvernementaux, mais aussi pour rassembler tous les acteurs des centres opérationnels ministériels afin de mieux travailler ensemble.

Des formats d'exercice

De cette approche interministérielle, il est nécessaire de décliner une programmation d'exercices également en interne pour entraîner et former nos collaborateurs, pour lesquels la gestion de la crise et l'application des plans ne sont pas leur quotidien. Cela peut passer par trois types :

- Un **exercice majeur interne** avec un scénario préparé à l'avance qui va mobiliser les acteurs de crise sur 1 ou 2 jours en testant les capacités d'armement des cellules de crise, le partage d'informations et les solutions à prendre pour sortir de la crise;
- Un **stress test**, qui est un format plus concis, sur quelques heures, et qui a pour objectif de se focaliser uniquement sur une ou deux procédures à tester : activation d'une cellule de crise, alerte des collaborateurs, conception d'un point de situation;
- Un **test technique**, qui, lui, peut durer de quelques heures à une journée, et qui va se focaliser uniquement sur un secteur d'activité particulier : informatique, logistique, sécurité bâtimentaire, communication, etc.

Une programmation partagée et adaptée

L'ensemble de ces temps d'exercice constitue une programmation qui doit être partagée avec sa communauté et adaptée en fonction des besoins de chacun. L'adhésion des parties prenantes à cette programmation est primordiale pour assurer leur participation.

Chaque crise a un impact sur l'une des quatre briques constituant les PCA :

- L'indisponibilité des bâtiments;
- L'indisponibilité des ressources humaines;
- L'indisponibilité des ressources informatiques;
- L'indisponibilité des partenaires.

"Se réunir est un début, rester ensemble est un progrès, travailler ensemble est la réussite. "

Henry Ford

En définitive, pour illustrer au mieux l'utilité d'un PCA et pour tester en situation « quasi » réelle les solutions imaginées au préalable, il est recommandé de décliner les exercices mentionnés précédemment avec des aspects « continuité d'activité ». Cette méthode incitera les structures de crise à réfléchir à des solutions dans leur globalité, incluant la continuité de leur activité, et non seulement à se focaliser uniquement sur la résolution d'une crise.

Pour concrétiser ce lien étroit entre la continuité d'activité et la gestion de crise, il peut être bénéfique de prévoir en amont, dans une maquette de point de situation, une partie réservée à la continuité d'activité. Cela amène le directeur de la gestion de crise, souvent pris par l'effervescence de la gestion d'une crise, à ne pas omettre d'inclure cet aspect dans sa réflexion globale; l'anticipation de la reprise d'activité étant un paramètre tout aussi primordial que la gestion de l'urgence des conséquences de la crise.

2. Le PCA seul n'est rien s'il n'est pas mis en adéquation avec ceux des partenaires

La réalisation d'un PCA peut amener un biais qui est de ne penser qu'au travers du spectre de sa structure, d'identifier et d'analyser uniquement son organisation interne en omettant les interactions avec ses partenaires.

Ainsi, la réalisation d'une cartographie des partenaires, tout comme il est nécessaire de faire une cartographie des acteurs pour la gestion de crises, est essentielle. Elle permet d'identifier les partenaires internes et externes et les prestataires avec lesquels il est important de maintenir le lien pour pouvoir continuer ses activités.

Sun Tzu décrivait ces interdépendances dans sa citation :

« Qui connaît l'autre et se connaît lui-même, peut livrer cent batailles sans jamais être en péril.

Qui ne connaît pas l'autre mais se connaît lui-même, pour chaque victoire, connaîtra une défaite.

Qui ne connaît ni l'autre ni lui-même, perdra inéluctablement toutes les batailles. »

Connaître le fonctionnement des partenaires

Il faut retenir ici que, pour pouvoir appréhender favorablement les nombreux événements qui vont impacter notre organisation interne, il est nécessaire de bien connaître le fonctionnement de ses partenaires également. Collectivement, il sera plus aisé dans un mode de fonctionnement dégradé de trouver les bonnes solutions pour rétablir les activités.

Dans la gestion de crises, l'un des fondamentaux est de bien connaître les autres acteurs des structures de crises pour que, le jour J, les relations soient facilitées et que la constitution d'un annuaire de crise opérationnel soit efficiente.

Ainsi, dès lors que notre PCA est achevé et qu'il intègre une cartographie des partenaires, il est important de pouvoir créer le lien avec ces derniers pour s'assurer non seulement que leur plan vous identifie bien comme partenaire, mais aussi pour mettre en adéquation le DMIA (délai maximal d'interruption admissible) attribué à chacun. Indiquer dans son PCA qu'il est essentiel de rétablir le lien avec l'entreprise « alpha » sous trois heures n'est opérationnel que si le PCA de l'entreprise « alpha » permet une reprise de l'activité sous cette même contrainte. Alors, vous pourrez travailler des solutions de reprise d'activité communes et, notamment, des moyens de communication adaptés, qui pourront être testés dans le cadre d'une programmation d'exercices commune.

3. Le PCA est vivant et doit être nourri régulièrement

Tout comme une belle plantation, un PCA, ça s'entretient avec de bons outils (SI adaptés), des compétences spécifiques (acteurs formés et entraînés), de l'engrais (mises à jour régulières) et des coupes et des repousses (adaptations aux retours d'expérience).

Votre PCA doit pouvoir s'enrichir des expériences vécues, s'adapter aux nouveaux défis de votre structure (nouvelles missions, réorganisations, évolution des effectifs), s'adapter aux nouvelles technologies (robotisation de certaines missions, nouveaux systèmes d'information, intégration de l'intelligence artificielle dans vos processus).

Les mises à jour

Votre démarche de continuité d'activité doit donc avoir une bonne hygiène de vie pour permettre et prévoir sa mise à jour. Tout comme il est désormais commun de réaliser un retour d'expérience à la fin d'un exercice ou de la gestion d'une crise, il est nécessaire de prévoir un retour d'expérience dès lors qu'une composante de votre PCA a été activée.

Finalement, il n'y a pas de modèle type de PCA. L'important est que le document que vous allez produire vous corresponde et surtout qu'il vous permette dans une période de stress où le temps est resserré, de rapidement retrouver les informations qui vous seront utiles. Ainsi, il est intéressant de pouvoir s'inspirer des présentations, des documents et des procédures que d'autres structures ont pu développer. La communauté de continuité d'activité évoquée précédemment n'est donc pas uniquement un enjeu interne, mais également un enjeu externe plus global. Promouvoir son PCA, le confronter à des regards externes et accepter qu'il puisse évoluer sont les gages de réussite de sa démarche de continuité d'activité.

La technologie au service de la résilience des entreprises

Interview

Benoit Froment

Expert en gestion de crises et résilience
Outils technologiques pour la gestion de la résilience

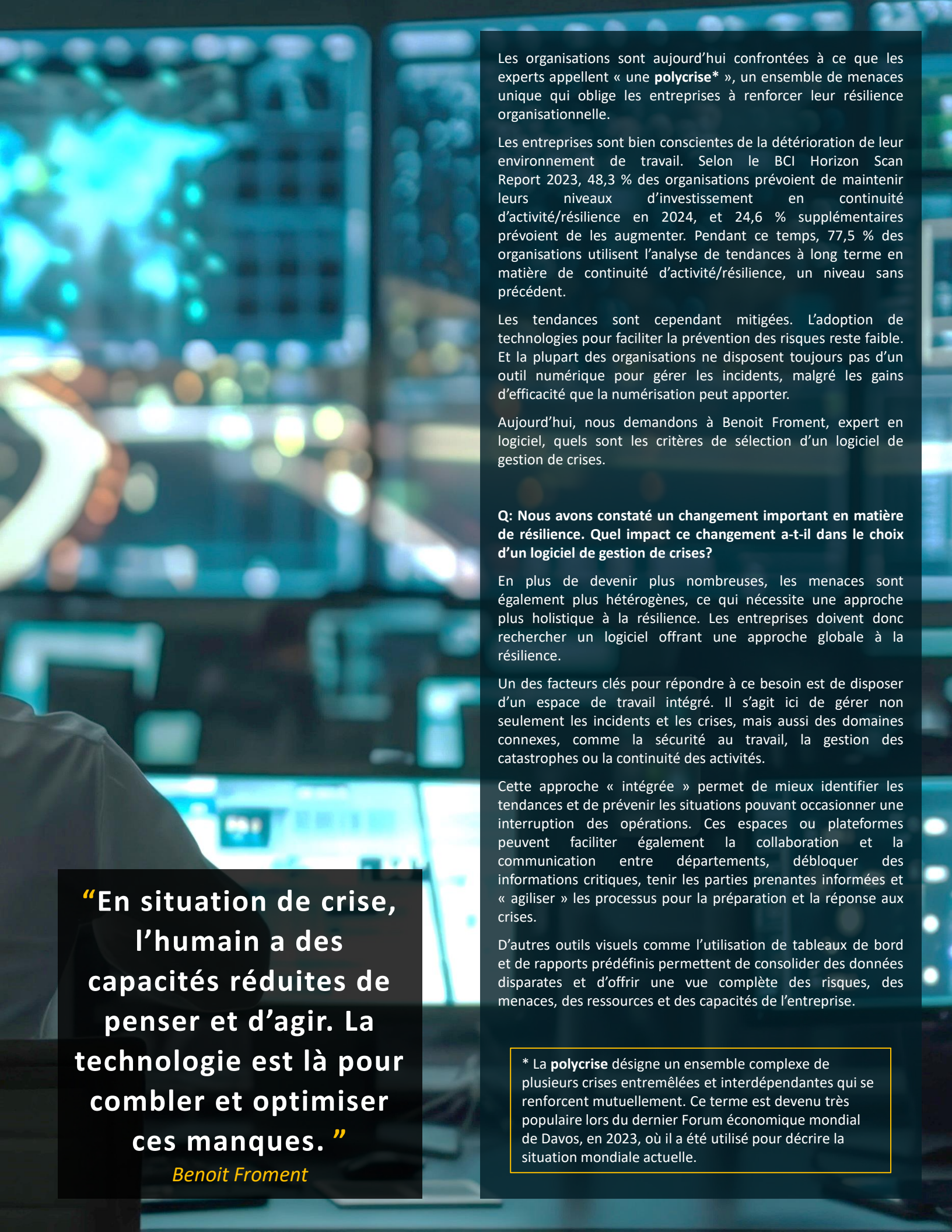
Nous traversons une ère de polycrise*.

La question est de savoir s'il existe des outils technologiques pour faire face à cet environnement.

L'entretien suivant permet d'identifier certains critères à prendre en compte pour choisir un logiciel de gestion de crises qui doit aider à planifier, à coordonner et à rationaliser les réponses aux crises et garantir la résilience de l'organisation.

Interview par Alexandre FOURNIER

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



Les organisations sont aujourd'hui confrontées à ce que les experts appellent « une **polycrise*** », un ensemble de menaces unique qui oblige les entreprises à renforcer leur résilience organisationnelle.

Les entreprises sont bien conscientes de la détérioration de leur environnement de travail. Selon le BCI Horizon Scan Report 2023, 48,3 % des organisations prévoient de maintenir leurs niveaux d'investissement en continuité d'activité/résilience en 2024, et 24,6 % supplémentaires prévoient de les augmenter. Pendant ce temps, 77,5 % des organisations utilisent l'analyse de tendances à long terme en matière de continuité d'activité/résilience, un niveau sans précédent.

Les tendances sont cependant mitigées. L'adoption de technologies pour faciliter la prévention des risques reste faible. Et la plupart des organisations ne disposent toujours pas d'un outil numérique pour gérer les incidents, malgré les gains d'efficacité que la numérisation peut apporter.

Aujourd'hui, nous demandons à Benoit Froment, expert en logiciel, quels sont les critères de sélection d'un logiciel de gestion de crises.

Q: Nous avons constaté un changement important en matière de résilience. Quel impact ce changement a-t-il dans le choix d'un logiciel de gestion de crises?

En plus de devenir plus nombreuses, les menaces sont également plus hétérogènes, ce qui nécessite une approche plus holistique à la résilience. Les entreprises doivent donc rechercher un logiciel offrant une approche globale à la résilience.

Un des facteurs clés pour répondre à ce besoin est de disposer d'un espace de travail intégré. Il s'agit ici de gérer non seulement les incidents et les crises, mais aussi des domaines connexes, comme la sécurité au travail, la gestion des catastrophes ou la continuité des activités.

Cette approche « intégrée » permet de mieux identifier les tendances et de prévenir les situations pouvant occasionner une interruption des opérations. Ces espaces ou plateformes peuvent faciliter également la collaboration et la communication entre départements, débloquer des informations critiques, tenir les parties prenantes informées et « agiliser » les processus pour la préparation et la réponse aux crises.

D'autres outils visuels comme l'utilisation de tableaux de bord et de rapports prédéfinis permettent de consolider des données disparates et d'offrir une vue complète des risques, des menaces, des ressources et des capacités de l'entreprise.

"En situation de crise, l'humain a des capacités réduites de penser et d'agir. La technologie est là pour combler et optimiser ces manques."

Benoit Froment

* La **polycrise** désigne un ensemble complexe de plusieurs crises entremêlées et interdépendantes qui se renforcent mutuellement. Ce terme est devenu très populaire lors du dernier Forum économique mondial de Davos, en 2023, où il a été utilisé pour décrire la situation mondiale actuelle.

Q: La fréquence des crises s'accélère aussi. Quelle fonctionnalité doit-on considérer pour relever ce défi?

Une réponse efficace aux incidents est nécessaire. La capture numérique de l'incident et l'automatisation de sa réponse doivent permettre aux équipes d'intervenir plus rapidement.

Une activation automatisée du plan de réponse à l'incident réduit le temps de réponse dans les situations critiques. Le plan (ou playbook) est activé automatiquement dès que l'incident est enregistré. Les personnes potentiellement touchées ou les équipes qui doivent participer au plan d'action sont informées sur-le-champ.

Q: Quelles avancées technologiques voyez-vous pour optimiser les communications en cas de crise?

Nous avons constaté un intérêt pour des plateformes ou des logiciels prééquipés de modèles de notifications ou de messageries, et accompagnés de processus d'affaires personnalisables. Ils permettent aux intervenants de préorganiser les communications et de préassigner certaines tâches, ce qui réduit considérablement les efforts manuels et les interventions humaines et augmente la fiabilité des communications.

Dans certains cas, il existe également des communications que l'on peut cibler, selon le rôle de la personne ou sa localisation, par exemple. L'objectif est de cibler les personnes potentiellement touchées par l'incident ou celles qui peuvent y répondre.

Q: La préparation aux crises devient elle-même plus complexe vu que les menaces possibles ne cessent d'évoluer et d'augmenter. Que recommandez-vous dans ce cas de figure?

Il y a deux fonctionnalités que l'on peut mentionner.

- La première est la possibilité de créer votre propre plan de réponse à une crise. Ce plan doit vous permettre de rapidement décrire la stratégie à appliquer et d'avoir accès à une première checklist d'actions à entreprendre en cas de crise. Cette checklist varie en fonction du scénario que l'on veut couvrir.
- La deuxième est d'utiliser des plans prédéfinis. Certains logiciels viennent équipés de plans, ou playbooks, développés à partir des bonnes pratiques de l'industrie. On y gagne énormément de temps.

Au bout du compte, la flexibilité de l'outil doit vous permettre de couvrir ces deux aspects.

Q: Un des risques est de se retrouver avec une multitude de plans à tester. Comment y faire face?

Vous avez raison. Ce que nous voulons éviter, ce sont des organisations qui attendent une crise réelle pour tester leurs plans, car elles en ont trop à tester.

L'outil que vous utiliserez doit proposer une fonctionnalité pour tester ces scénarios en conditions réelles. Lors d'un exercice virtuel, l'outil doit pouvoir indiquer étape par étape les bonnes pratiques à suivre. L'utilisateur doit se sentir à l'aise non seulement avec le processus à suivre, mais aussi avec l'interface en elle-même.

La polycrise, cette accumulation d'événements critiques simultanés et leur durée, oblige les entreprises à renforcer leur résilience comme jamais auparavant.

Ce renforcement peut être accompagné d'une composante technologique. De plus en plus d'entreprises choisissent d'investir dans des logiciels de gestion de crises ou de continuité d'activité.

Ces outils permettent d'automatiser un certain nombre de processus, d'améliorer la préparation aux crises et d'optimiser leur réponse.

En situation de crise, l'humain a des capacités réduites de penser et d'agir. La technologie est là pour combler et optimiser ces manques.

Interview de Benoit Froment

Benoit est Expert en technologies de l'information avec plus de 20 ans d'expérience mettant en place des solutions logicielles pour la résilience des entreprises, la gestion de crises, la continuité des activités et les opérations de sécurité physique et informatique. Il travaille pour l'entreprise NOGGIN.

Noggin est le leader australien dans le secteur de la technologie pour la gestion d'événements critiques avec sa plateforme logicielle cloud de nouvelle génération permettant d'identifier tout risque ou incident physique ou cyber, de s'y préparer, d'y répondre et de se remettre de l'incident. Nous gérons les perturbations plus intelligemment!

www.noggin.io

4 fonctionnalités clés dans la sélection d'un logiciel de gestion de crises

1. Adopter une approche intégrée

Les menaces deviennent plus nombreuses et diverses, nécessitant une approche globale de la résilience. Recherchez un logiciel avec un espace de travail de résilience intégré qui gère les crises, la santé-sécurité au travail, la protection des biens et des personnes, la gestion des urgences et des catastrophes, la continuité des activités et les risques.

2. Automatiser la réponse aux incidents

Les crises deviennent plus complexes et rapides. Un logiciel avec des capacités de réponse automatisée aux incidents est essentiel. Ce type de logiciel peut réduire considérablement les temps de réponse en automatisant instantanément les scénarios et en appliquant le plan approprié à chaque incident.

3. Rendre la planification dynamique

Avec la complexité croissante de la gestion de crises, le logiciel doit intégrer de manière transparente toutes les données stockées et inclure les meilleures pratiques de l'industrie. Cela permet aux organisations de générer des plans de réponse aux crises et aux incidents adaptés aux scénarios de menace changeants.

4. Simplifier la gestion des exercices

Les plans de gestion de crises doivent être testés et intégrés pour être efficaces. Choisissez un outil qui guide les utilisateurs à travers chaque étape d'un exercice, en veillant à ce que tous les participants comprennent leurs rôles et les étapes à suivre. Cela permet de garder les plans prêts à l'action.

Source : https://www.noggin.io/blog/4-capabilities-to-consider-in-selecting-crisis-management-software

Responsable de la sécurité de l'information ou de la résilience de l'entreprise?

Depuis 15 ans, j'ai vu changer mon métier. Il y a 15 ans, pas de ransomware, pas de télétravail.

Le mot « cybersécurité » n'était pas à la mode et la résilience, pas dans mon vocabulaire.

Aujourd'hui, le besoin a changé, mon métier a changé.

Par Maxime Gryl

Expert en cybersécurité freelance. RSSI à temps partagé.

J'aide les entreprises à gagner en sérénité avec leur cybersécurité. Je m'occupe de la gouvernance de la sécurité de l'information.

Dix-huit ans d'expérience. Mon métier a changé, ou j'ai changé mon métier.

Suis-je toujours RSSI, responsable de la sécurité des systèmes d'information chargé de la cybersécurité? Ou un service de soutien au bon fonctionnement de l'entreprise?

La sauvegarde? Ce n'est pas de la cyber!

C'est ce qu'on disait il y a 15 ans entre collègues ingénieurs en sécurité informatique, à une époque où le mot « cyber » n'était pas encore à la mode. Et bien que nous reconnaissions l'intérêt de la maîtrise de la sauvegarde par la sécurité, en pratique, il y avait peu d'échanges avec l'équipe responsable des sauvegardes, qui travaillait de manière autonome pour des besoins fonctionnels ou normatifs.

Alors pourquoi aujourd'hui la première mission que j'ai en tête quand je suis responsable de la sécurité, c'est la sauvegarde, la résilience, la survie de l'entreprise?

Ce sont d'ailleurs mes premières questions quand je rencontre un responsable de PME : « Avez-vous des sauvegardes? », puis « Avez-vous testé les procédures de restauration? », bien que je reste souvent sceptique quant à la véracité des réponses obtenues.

Le ransomware qui change la donne

Cette bascule pour moi s'est faite avec l'ingénieuse invention du ransomware.

Je me souviens de l'admiration profonde que j'ai eue pour le petit génie qui a un jour mis en place l'extorsion à la donnée informatisée… T'empêcher d'utiliser TES données et te demander de l'argent pour récupérer ce qui est déjà à toi.

Mais surtout, le ransomware, c'était la garantie que, quand il était exécuté, on avait perdu. Pas de retour en arrière sans rançon… ou sauvegardes!

Notre travail quotidien de renforcement de la sécurité ne servait plus à rien si la – forcément toujours présente – dernière petite faille était exploitée par un bon ransomware…

L'indisponibilité au centre, on découvre la dépendance

À se rendre compte des impacts d'un ransomware, on concentre notre travail sur les risques de perte de disponibilité de l'information, ou de perte complète. Et nous voilà à nous rendre compte de la dépendance au numérique.

Et de la dépendance du numérique à beaucoup d'autres choses…
Le métier reprend un virage quand, au lieu de lutter contre « les méchants hackeurs russes ou chinois » avec plein de technologies cyber, on se voit lutter contre un risque d'intrusion de force 9 parce que la porte de secours ne ferme plus…

Mais quelles sont les limites du périmètre du RSSI?

Il y a 10 ans, un collègue RSSI d'une banque française me disait :

« Je suis RSSI, pas CISO; c'est-à-dire chargé de la sécurité du système d'information, pas de l'information. Je suis responsable de ton document, là, dans ta boîte mail, mais, si tu l'imprimes, alors je considère que ce n'est plus mon problème… ».

L'évidence est là, on ne peut pas mettre sous le tapis une partie du système sous prétexte que l'on considère que ce n'est plus numérique ou que c'est la responsabilité de quelqu'un d'autre. Le bâtiment et ses accès physiques, le télétravail, la téléphonie, la formation, le papier, la vieille application métier, etc. : les risques doivent être connus et mesurés, et quand ils sont délégués, cette délégation doit être maîtrisée.

Compréhension transversale

En cherchant à protéger l'entreprise, en prenant du recul et en comprenant la dépendance au numérique, la posture holistique s'impose, plaçant la résilience au centre de la stratégie.

Cette réalité numérique transforme la survie de l'entreprise en un enjeu stratégique majeur. Face à cette mutation, mon rôle en tant que RSSI a dû évoluer significativement.

Ainsi, comprendre en profondeur les enjeux stratégiques de l'entreprise et interagir avec le conseil d'administration sont devenus des composantes essentielles de mes responsabilités. Il est impératif que je m'assure que la direction comprend les risques et les menaces, non seulement pour garantir la conformité aux normes et aux réglementations, mais aussi pour préserver la pérennité et le développement de l'entreprise.

(Re)cadrage en cours

C'est d'ailleurs ce que proposent les référentiels – ô guides supposés du bien-faire – comme NIS2, ISO 27001 ou le règlement DORA, qui exigent l'engagement formel de la direction de l'entreprise, une cartographie de ses risques et le management ferme de ses prestataires de services critiques.

Et en prenant une approche de gestion de la sécurité plutôt que des référentiels techniques, ces normes démontrent l'importance d'une gouvernance holistique bien au-delà des aspects techniques.

Me voilà responsable que tout fonctionne tout le temps?

Quelle douce illusion, flattant mon ego, que de croire que l'entreprise tient bon grâce à moi. Quelle belle cape je feins d'endosser, bien qu'elle me semble un peu moins reluisante que celle du « policier des ordinateurs » quand je l'explique à ma fille de 6 ans.

J'ai hâte de voir ces prochaines années comment le métier changera encore; l'IA, le cloud à outrance, les normes, les guerres cyber… De quoi repenser les besoins de nos chères entreprises, qui vont naturellement transformer nos missions.

Le métier évolue. Je constate aujourd'hui que de nombreux jeunes aspirent à devenir « des hackeurs éthiques », experts techniques. Cependant, une partie significative des besoins réels se concentre sur l'accompagnement à la croissance de l'entreprise.

Ce fut le cas pour les directions des systèmes d'information (DSI), qui sont passées de simples « offreurs techniques » à partenaires et à accélérateurs du métier. La cyber connaîtra sa transformation.

À présent, la question se pose pour vous : considérez-vous les services d'un garagiste comme de simples prestations de maintenance, pour la vidange ou le montage de pneus, ou comme l'expertise d'un professionnel qui veille à la santé de votre véhicule pour garantir sa longévité et votre sécurité?

Maxime Gryl

MGR SOLUTIONS

Expert cyber depuis plus de 18 ans. Après le secteur bancaire, la santé et l'infogérance TI, je suis devenu expert freelance pour mieux travailler avec les entreprises en quête de sérénité et d'organisation de leur cybersérénité.

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

Posez-vous les bonnes questions sur la place de votre (R)SSI

Voici des pistes de réflexion pour challenger la place de la cyber et de votre RSSI dans votre stratégie. N'hésitez pas à titiller votre responsable : un RSSI est expert en gestion du risque, et le premier à se protéger! (Ou non, le deuxième après le juriste.)

Côté business :

- Quels marchés nouveaux pourrions-nous atteindre avec un niveau de sécurité ou avec une certification supplémentaire?
- Être meilleur en cyber et le montrer nous donnerait-il un avantage par rapport à nos concurrents?
- La conformité a tendance à être conservatrice; si tu avais des objectifs de croissance pour l'entreprise, quels risques serais-tu prêt à concéder?

Côté niveau de sécurité :

- Quelles sont les trois principales préoccupations en matière de sécurité que tu ne communiques pas toujours en réunion?
- Y a-t-il un sujet que tu n'abordes que pour tenir tes objectifs, mais qui mériterait d'être revu pour être en cohérence avec le reste?
- Pour une sécurité à 5 ou 10 ans, nous sommes dans le bon sens ou nous creusons le gap?

Côté organisation :

- Avec quelles équipes t'entends-tu le moins ou te sens-tu en concurrence? Comment faire pour vous réaligner sur les objectifs de l'entreprise, moins vous ralentir et accélérer dans le bon sens?
- Avec quelles équipes pourrions-nous rationaliser les coûts cyber? La production pour les machines, la qualité pour les processus, le management pour la sensibilisation?
- Sûreté, résilience, sécurité… des mondes qui se rapprochent mais qui ne se parlent pas toujours. Si tu étais responsable de l'ensemble de ces sujets, quel domaine te semblerait le moins maîtrisé?

Pour le pousser dans ses derniers retranchements :

- Si demain nous avions une proposition de rachat de l'entreprise, le diagnostic cyber des investisseurs serait-il une aide ou un frein à la vente?
- Gérer la conformité et gérer une crise, ce n'est pas pareil. En cas de crise, peux-tu la gérer ou il est judicieux de se préparer autrement?
- S'il y a une attaque ou une malveillance demain, saurais-tu témoigner devant un tribunal pour dire que tout était fait comme cela devait être?

PRA spécial TPE/PME : simple, efficace et accessible

Les TPE/PME n'ont pas le temps ni les moyens de sécuriser leur entreprise.

Pourtant, l'adage dit bien :

la cybersécurité avant, c'est trop cher; après, c'est trop tard.

Changeons les règles en leur proposant un Plan de Reprise d'Activité (PRA) simple et efficace, synonyme de résilience face aux cybermenaces.

Par Pierre-Alban Maurin

Responsable de BU Cybersécurité

Nous proposons des offres cyber spécifiquement conçues pour les TPE/PME (SOC humain 24/7, audits, mise en conformité…).

Il est difficile de catégoriser toutes les TPE/PME de manière uniforme. En effet, une start-up composée de cinq personnes travaillant dans le domaine nucléaire n'aura pas les mêmes priorités en matière de PRA qu'une PME agroalimentaire comptant 200 employés.

Nous allons voir comment mettre en place un PRA sur mesure qui puisse correspondre à un grand nombre d'entre elles.

Revenons-en aux fondements de la norme ISO 22301, qui assure la continuité d'activité en cas d'incidents. À l'instar des autres normes de sécurité connues, une bonne définition du contexte est primordiale.

Le contexte

Le marché SMB possède un avantage significatif par rapport aux grosses entreprises sur ce plan. Les rapports humains y sont plus faciles, les différents services moins cloisonnés et le taux de turn-over généralement moins élevé. Il est alors plus aisé pour un certain nombre de collaborateurs d'avoir une vision exhaustive et globale du contexte de leur entreprise.

Comprendre en profondeur l'organisation, ses processus, ses activités critiques, les parties prenantes et l'environnement concurrentiel et réglementaire constitue les fondements de la reprise d'activité. Il s'agit d'identifier l'essence même de cette dernière pour pouvoir la reprendre au plus vite après un incident.

Il est nécessaire d'envisager comment un incident pourrait survenir. À défaut d'une analyse de risques complète, nous pouvons ici nous poser quelques questions de base :

- **Quels sont les biens dits « essentiels » de mon entreprise?** Ces éléments peuvent être définis comme des actifs, des processus, une fonction critique, des données... Ils jouent un rôle crucial dans le fonctionnement de l'organisation, et leur préservation est indispensable pour assurer la continuité des activités.
- **Sur quels supports reposent ces biens essentiels?** Il s'agit ici des supports physiques ou humains, tels qu'un serveur, un pare-feu, un coffre-fort ou un employé. Ce n'est pas le coffre en soi que vise le cambrioleur, mais l'argent à l'intérieur. Mais pour l'obtenir, notre voleur devra concentrer toute son énergie sur le contenant et non le contenu.

Pour minimiser le risque de cessation d'activité, il est nécessaire de redonder les biens supports contenant des données critiques pour l'entreprise. N'oublions pas les collaborateurs, en particulier dans le contexte des PME, où souvent un seul employé a accès à certaines ressources.

Une bonne compréhension du contexte permet donc de déterminer les données essentielles pour l'entreprise. Une fois qu'elles sont collectées, il convient de les sauvegarder régulièrement.

La sauvegarde

Une pratique bien connue dans ce domaine est celle du 3-2-1 :

- **3** copies des données;
- **2** sur un support différent (un disque dur chiffré dans un coffre-fort et un serveur de stockage, par exemple);
- **1** sauvegarde hors site.

Le stockage des données peut malheureusement être coûteux. Ces données sont en effet ce que vous avez de plus sensible et il convient de ne pas les laisser à n'importe qui. Vous aurez alors tendance à vouloir choisir un hébergeur souverain, ultrasécurisé et bardé de certifications. Mais alors le prix sera vite rédhibitoire.

Une solution de rechange sera de stocker les données dans une archive chiffrée. Une méthode de chiffrement robuste telle que l'AES 256 et un mot de passe fort seront les garants de votre confidentialité.

Vous pourrez alors en toute quiétude mettre votre archive chez un hébergeur plus abordable financièrement.

Une deuxième copie des données peut être stockée sur un disque dur chiffré, tandis qu'une troisième peut être conservée sur un serveur de fichiers. Il est essentiel de gérer de manière sécurisée les mots de passe et les clés de chiffrement, en les conservant dans un lieu sûr, comme un coffre-fort numérique.

Une fois ces données mises en sûreté, il faut déterminer nos métriques.

Le recovery point objective (RPO) correspond à la perte de données maximale admissible. Par exemple, si mes sauvegardes sont effectuées toutes les 24 h, j'accepte, au pire, de perdre 23 h 59 min de données.

Il est ensuite nécessaire de définir la durée d'interruption maximale admissible, appelée return time objective (RTO). Il faudra alors faire en sorte de pouvoir restaurer les sauvegardes durant le laps de temps défini, même si cela signifie fonctionner temporairement en mode dégradé.

Voir schéma de synthèse ci-dessous

La reprise de l'activité

Que l'interruption de l'activité soit intentionnelle ou non, tous les efforts sont déployés pour éviter qu'elle ne se produise. Un incident peut malgré tout survenir. Il sera certes traité différemment selon sa nature. Cependant, certaines étapes sont communes : identifier la cause, évaluer les conséquences et, en fonction de celles-ci, restaurer les sauvegardes.

En cas de cyberattaque, il sera nécessaire d'investiguer pour s'assurer que cette dernière a bien été endiguée. Pour ce faire, il est essentiel d'isoler le réseau de l'entreprise d'Internet et de mener des analyses pour neutraliser la menace. Il est probable que, dans ce cas, les sauvegardes locales, voire en mode logiciel-service SaaS, soient compromises. Dans ce cas, celles du disque dur prennent le relais.

La nécessité d'une reprise d'activité découle de cette réalité implacable :

Personne n'est à l'abri d'une cyberattaque.

C'est un peu comme un motard qui roule tous les jours pendant 40 ans. À un moment donné, le risque de chute devient presque inévitable. Dans ce contexte, la reprise d'activité joue le rôle d'équipement de protection et de tampons antichute pour atténuer les conséquences d'une chute et permettre au motard de reprendre la route rapidement.

Ainsi, mettre en place un PRA efficace et isoler correctement ses sauvegardes permettra à une entreprise de reprendre ses activités le plus rapidement possible.

Pierre-Alban Maurin

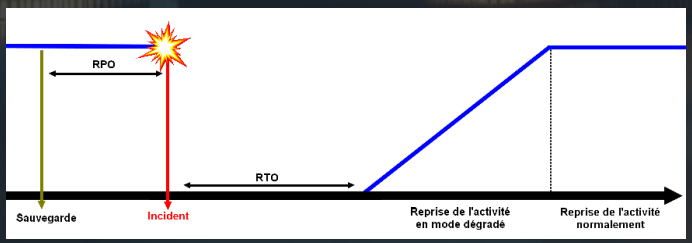


Schéma synthèse

10 clés pour mettre en œuvre son PRA simplifié

- Lister toutes les données cruciales à mon entreprise pour la reprise d'activité.
- Mettre toutes ces données dans une archive chiffrée et cette dernière dans le cloud.
- Les mettre également dans un disque dur chiffré, ce dernier étant à mettre en lieu sûr.
- Les mettre enfin dans un serveur de fichier ou autre stockage en local.
- Définir sa perte de données maximale admissible (recovery point objective en anglais). Effectuer les sauvegardes en conséquence, et ce, régulièrement. Par exemple, je ne peux pas me permettre de perdre plus de trois jours de travail pour la survie de mon entreprise. Je vais donc définir mon RPO à 72 h et mettre à jour mes sauvegardes tous les trois jours.
- Définir ma durée d'interruption maximale autorisée (return time objective en anglais). S'entrainer régulièrement à restaurer les sauvegardes durant ce laps de temps. Définir également, si besoin, un délai d'intervention du prestataire en cybersécurité en adéquation avec le RTO pour les besoins des investigations numériques.
- En cas d'incident, trouver la cause et évaluer les conséquences.
- Si l'incident est dû à une cyberattaque, commencer par isoler le réseau d'Internet.
- Mener ou faire mener les investigations numériques pour neutraliser la menace.
- Restaurer les sauvegardes une fois l'attaque endiguée.

Méthode des 3 sphères pour renforcer la résilience en entreprise

Découvrez comment aligner les sphères organisationnelle, fonctionnelle et technique pour renforcer la résilience de votre infrastructure informatique.

Par Stéphane Atlani

Directeur des systèmes d'information à temps partagé

Stratégie information et business. J'interviens aussi sur des sujets d'urgence ou en gestion de crise.

La résilience en gestion de crise est la capacité d'une organisation à anticiper des perturbations, à s'y préparer, à y répondre et à s'en remettre rapidement. Cet article explore comment les entreprises peuvent renforcer leur résilience en se concentrant sur trois sphères informatiques interdépendantes : technique, fonctionnelle et organisationnelle.

Cette méthodologie est le fruit de plus de mes 20 ans d'expérience dans le domaine de l'informatique et de la gestion des entreprises.

Les différentes sphères informatiques

Dans le monde de l'informatique, nous retrouvons les grands domaines suivants :

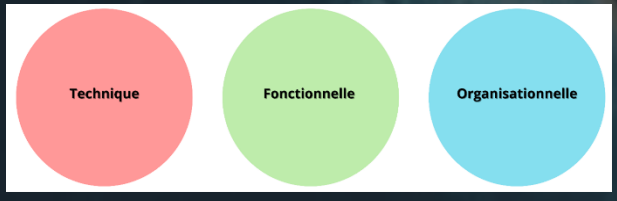
- Le système informatique ou le système d'information, qui comprend les ordinateurs, les serveurs, les réseaux et les logiciels;
- La programmation, dont l'objectif est l'écriture de logiciels et d'applications;
- La sécurité informatique, dont l'objectif est de garantir la protection des systèmes d'information;
- La science des données, qui analyse et interprète les grands ensembles de données;
- Les autres domaines, comme la robotique, la bio-informatique, l'informatique quantique et l'intelligence artificielle.

Tous ces domaines interagissent entre eux. Par exemple, la science des données ne serait rien sans la programmation, qui permet le développement des applications utilisées par la science des données, et elle-même ne serait rien sans le système d'information, qui permet de disposer des matériels et des réseaux afin de collecter, de stocker, de traiter et de distribuer de l'information.

Mais ce n'est pas tout : le domaine de l'intelligence artificielle ne serait rien sans la science des données.

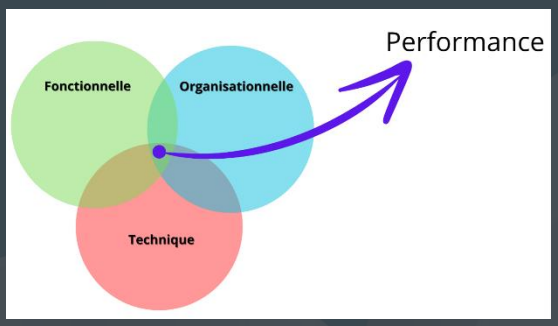
Dans chacun de ces domaines, vous trouverez de l'organisation, de la gouvernance, de la stratégie, de la fonctionnalité et de la technique. C'est le concept des trois sphères :

- La sphère organisationnelle est celle où nous retrouvons la stratégie, la gouvernance et, bien sûr, l'organisation. En gros, c'est ici que nous décidons.
- La sphère fonctionnelle décrit comment doit fonctionner un élément et fait l'interaction entre la sphère organisationnelle et la sphère technique. C'est ici que nous imaginons.
- La sphère technique, c'est la partie technique, la main dans le cambouis. C'est ici que nous faisons.



Il n'existe pas une sphère plus importante qu'une autre; chaque sphère est importante et a son rôle.

Au milieu de l'alignement de ces trois sphères se trouve la performance.



Comment développer une résilience et aligner les trois sphères?

L'alignement des trois sphères et le développement de la résilience nécessitent une approche méthodologique et des priorités claires.

Chaque décision doit être prise de manière holistique, en tenant compte des impacts et des interactions entre les sphères techniques, fonctionnelle et organisationnelle. Voici quelques conseils pratiques pour y parvenir.

Évaluez et identifiez les risques : soyez conscient de vos vulnérabilités pour les renforcer efficacement.

Pour évaluer les risques, dressez un inventaire de vos ressources, effectuez des audits de sécurité réguliers et classez les vulnérabilités par priorité. Utilisez des outils de gestion des risques pour visualiser les menaces et leur interdépendance. Simulez des scénarios de crise pour comprendre les impacts et préparer des réponses appropriées. Une vulnérabilité peut perturber les processus métier et affecter la gestion des ressources.

Élaborez un plan de continuité et de réponse aux crises : préparez-vous à l'imprévisible en planifiant méticuleusement.

Pour élaborer des plans de continuité et de réponse aux crises, intégrez les aspects techniques, fonctionnels et organisationnels dans vos plans. Incluez des protocoles pour maintenir les activités essentielles malgré les perturbations. Organisez des simulations de crise régulières pour tester l'efficacité des plans. Développez des plans de réponse aux incidents pour chaque sphère et formez les équipes à réagir efficacement. Un plan de continuité technique doit être soutenu par des processus fonctionnels clairs et une structure organisationnelle réactive.

Automatisez pour être résilient : automatisez pour anticiper et réagir plus rapidement.

Pour renforcer la résilience, utilisez des outils d'automatisation pour les tâches répétitives et critiques, réduisant la dépendance humaine et minimisant les erreurs. Adoptez des technologies de surveillance proactive pour détecter les anomalies en temps réel. Investissez dans des infrastructures cloud sécurisées et des solutions de cybersécurité avancées. Mettez en place un programme de maintenance proactive et appliquez les correctifs de sécurité rapidement. L'automatisation doit soutenir les processus fonctionnels et être intégrée dans la structure organisationnelle, avec des systèmes de monitoring alertant toutes les équipes pour une réaction coordonnée.

Miniguide pour développer une résilience avec la méthode des 3 sphères

L'alignement des trois sphères – technique, fonctionnelle et organisationnelle – est crucial pour une résilience efficace.

Voici un guide pratique pour vous aider à mettre en œuvre cette méthode.

Évaluation et identification des risques

Commencez par dresser un inventaire complet de vos ressources, dont les matériels, les logiciels, les données et les réseaux. Effectuez des audits de sécurité réguliers pour identifier les points faibles. Classez ces vulnérabilités par ordre de priorité en fonction de leur impact potentiel. Utilisez des outils de gestion des risques pour visualiser les menaces et leur interdépendance entre les sphères. Simulez différents scénarios de crise pour comprendre les impacts et préparer des réponses appropriées.

Élaboration de plans de continuité et de réponse aux crises

Créez des plans de continuité des opérations (PCO) intégrant les aspects techniques, fonctionnels et organisationnels. Chaque plan doit inclure des protocoles pour maintenir les activités essentielles malgré les perturbations. Organisez des simulations de crise régulières pour tester l'efficacité des plans. Développez des plans de réponse aux incidents pour chaque sphère et formez les équipes à réagir efficacement.

Automatisation et technologies de surveillance

Utilisez des outils d'automatisation pour les tâches répétitives et critiques afin de réduire la dépendance humaine et de minimiser les erreurs. Adoptez des technologies de surveillance proactive pour détecter les anomalies en temps réel. Investissez dans des infrastructures cloud sécurisées et des solutions de cybersécurité avancées. Mettez en place un programme de maintenance proactive pour garder vos systèmes à jour et appliquez les correctifs de sécurité dès leur disponibilité.

La culture de la résilience : cultivez une culture de résilience où chaque employé est un gardien de la sécurité.

Donnez une vision de la résilience à vos collaborateurs : un bon capitaine se distingue par sa capacité à guider son navire à travers la tempête.

Pour un leadership et une gouvernance efficace, encouragez un leader qui anticipe les crises et prend des décisions proactives pour renforcer la résilience. Engagez les leaders dans les exercices de simulation de crise et les initiatives de formation. Établissez des comités de crise avec des représentants de chaque sphère pour une prise de décision rapide et coordonnée, dotés de ressources et de pouvoirs suffisants. Le leadership doit intégrer les perspectives des trois sphères, dont l'apport des experts techniques, fonctionnels et organisationnels, pour des décisions éclairées et pour une vision holistique.

Pour qu'une organisation soit véritablement résiliente, elle doit intégrer de manière cohérente les trois sphères : technique, fonctionnelle et organisationnelle. En investissant dans la résilience à travers ces trois dimensions et en prenant des décisions de manière holistique, les organisations peuvent non seulement survivre aux crises, mais aussi en ressortir plus fortes et mieux préparées pour l'avenir.

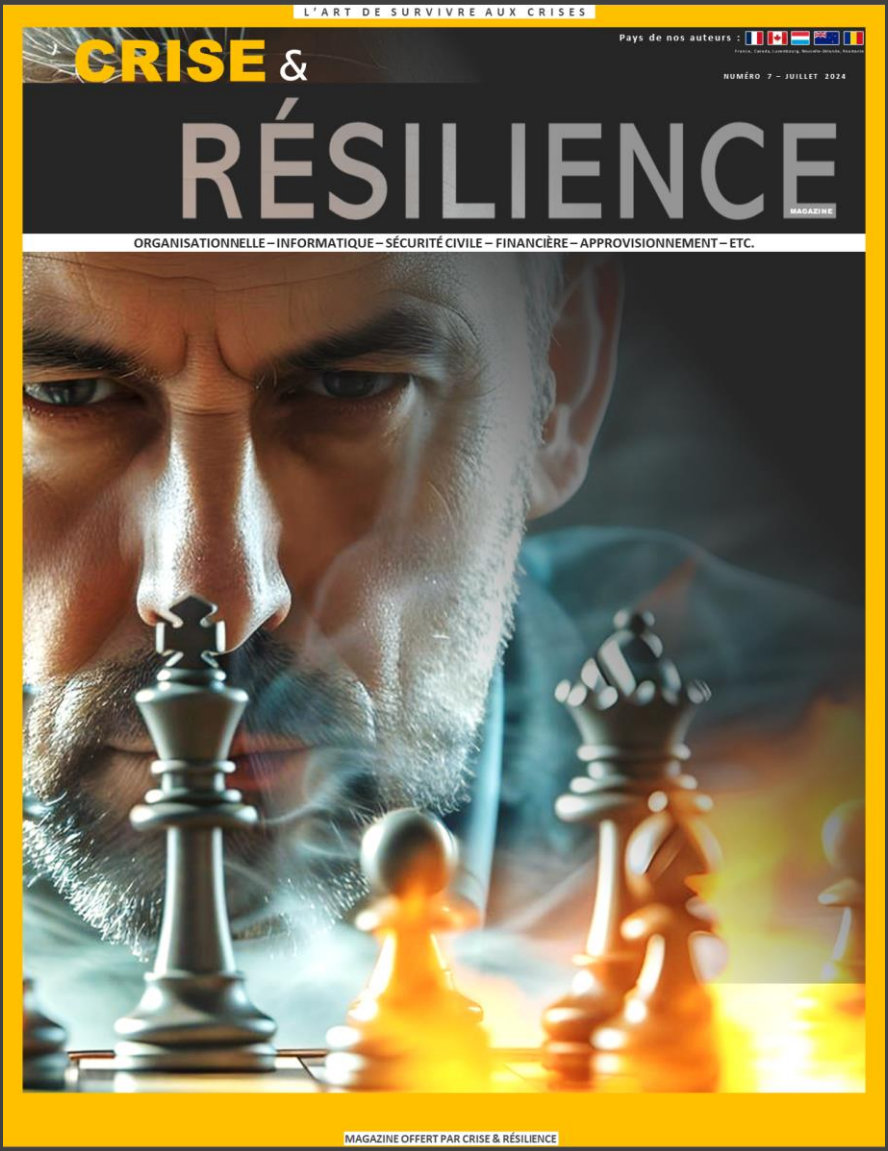
Stéphane Atlani

Starium
RÉVÉLEZ VOS TALENTS

Stéphane Atlani, DSI à temps partagé chez Starium et directeur associé chez Finaxim. Mon rôle est de donner de la valeur aux entreprises et de former les DSI de demain grâce à des solutions innovantes et abordables.

https://www.starium.xyz/accueil

RECEVEZ LE PROCHAIN MAGAZINE



Abonnez-vous

GRATUITEMENT

www.CriseEtResilience-Magazine.com