L'ART DE SURVIVRE AUX CRISES

CRISE & RÉSILIENCE MAGAZINE

Les auteurs des articles sont de

NUMÉRO 3 – JUILLET 2023

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

Résilience, la clé
de la prospérité dans un monde incertain

Cyber Terrorisme
et blanchiment d'argent

Efficacité opérationnelle
avec la digitalisation

Renforcer sa résilience
face aux risques cyber (Norme AFNOR)

PMU
l'importance et l'efficacité

Gestion de crise et intelligence artificielle
entre efficacité et limites

PARRAIN DE CE NUMÉRO

NICOLAS-LOÏC FORTIN

INTERVIEW :
LES ERREURS À ÉVITER LORS D'UNE CYBERATTAQUE ?

ISSN 9999-9999

DOSSIER DU MOIS

Gestion de la continuité des services dans les villes

CRISE &

RÉSILIENCE C'EST ... AUSSI

Une chaîne YouTube avec...

Des interviews d'experts :

Des réponses à vos questions :

Des conférences et formations gratuites

S'ABONNER ici

Une page LinkedIn avec...

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

Rejoignez-nous sur LinkedIn

EDITO DE NICOLAS-LOÏC FORTIN

Nicolas-Loïc Fortin
Conseiller stratégique

Fondateur de polysécure et cofondateur du **salon de cybersécurité séQCure**

C'est un honneur pour moi d'ouvrir cette nouvelle édition du magazine Crise & Résilience, une ressource inestimable pour tous ceux qui, comme moi, se passionnent à la compréhension et à la maîtrise des crises. Dans un interview, Alexandre Fournier m'a offert l'opportunité de partager mes réflexions et expériences sur la gestion de crise en cybersécurité. La résonance de cette conversation avec les sujets de l'édition actuelle est frappante.

Dans l'interview, j'ai souligné que la panique est l'ennemie de l'efficacité, que nous devons garder la tête froide, même face à la crise la plus dévastatrice. C'est cette sérénité, nourrie par une préparation adéquate, qui nous permet de prendre les meilleures décisions, guidées par la rationalité et non par l'émotion.

Dans ce numéro vous pourrez en apprendre plus sur un éventail riche et diversifié de thèmes, allant du témoignage sur la mise en place de communication de secours après le tremblement de terre d'Haïti en 2010, à l'exploration de la résilience, en passant par l'interface entre gestion de crise et intelligence artificielle. Il traite également de l'importance d'un PMU et de son opérationnalisation, des avantages et défis du cloud, et de l'amélioration de l'efficacité opérationnelle par la digitalisation. En outre, le numéro aborde les sujets épineux du cyberterrorisme et du blanchiment d'argent, tout en soulignant l'importance de la continuité des services pour les villes en temps de crise.

À travers ces thèmes, nous souhaitons aider à transformer une situation potentiellement dévastatrice en une opportunité de croissance et de renforcement. En fin de compte, la résilience est l'art de naviguer à travers les crises avec sérénité, prudence et détermination, pour émerger plus fort de l'autre côté.

sommaire

Numéro 3 – JUILLET 2023

ÉDITO DE LA RÉDACTION

Chers lecteurs et lectrices,

C'est avec une immense joie et une grande fierté que nous vous présentons notre troisième numéro ! Quelle aventure extraordinaire que de réaliser ce magazine pour vous, trimestre après trimestre. Nous sommes ravis de collaborer avec nos talentueux auteurs, qui partagent leurs passions et leur générosité sans compter à travers leurs articles captivants.

Dans ce numéro, le dossier du trimestre se concentre sur un sujet essentiel : comment aider les villes à maintenir leurs activités. Sujet d'actualité avec les récentes émeutes en France et les feux de forêt au Québec. Nous présentons des solutions qui peuvent être mises en place pour assurer la continuité des activités et favoriser la résilience des villes touchées.

Nous vous remercions pour votre soutien et votre fidélité qui nous encouragent à maintenir et à produire ce magazine chaque trimestre. Votre présence est une source d'inspiration et de motivation pour toute notre équipe.

Nous vous souhaitons une lecture chaleureuse et enrichissante.

Alexandre et Karine

Direction de la publication: Alexandre Fournier – Correction: Véronique Cyr – Création graphique: Alfo65 – Crédit photo: FreePix - Édition: **Crise&Résilience**-1624, rue de la Carrière-Vézina, Québec (Qc), Canada **Pour toute question: info@crise-resilience.com**

Rejoignez-nous sur **LinkedIn**

Dépôt légal: en cours – Numéro ISSN: en cours

SOYEZ RÉSILIENT

JANVIER – AVRIL – JUILLET – OCTOBRE

Rejoignez-nous sur **LinkedIn**

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

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

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

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

Et en plus, c'est gratuit!

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

Nous sommes fiers d'avoir apporté notre soutien au projet des étudiants de **l'École des Mines de Paris**.

Leur travail remarquable a été récompensé, avec leur projet

« Concevoir un guide de bonne pratique de continuité d'activité »

qui s'est classé premier parmi les projets présentés.

C'est une véritable réussite pour eux, et nous sommes heureux d'avoir pu contribuer à leur succès.

Félicitations à toute l'équipe !

MS ERC
400 abonnés
3 sem. • Modifié •

+ Suivre •••

Les Actes d'Entreprendre en Sécurité (AES) du MS ERC de Mines Paris correspondent à des projets en lien avec la prévention des risques et la gestion des crises. Ils sont menés en autonomie par les étudiants, constitués en groupes. Lucas Lenouvel, Roméo Perries, Walid Moustaghfir et Victor MALINCONI sont les lauréats de l'édition 2023.
Leur projet « Concevoir un guide de bonne pratique de continuité d'activité » a été classé premier par le jury, composé de Anne BUCK de PREVENTEO : SOLUTIONS LOGICIELLES QHSE - RH - CYBER - RSE, Audrey COLLE de Robertet Group, et Jerome Patte de Virbac.
Cet AES a été tutoré par Eric Rigaud, enseignant-chercheur à Mines Paris.

MINES PARIS | PSL
Centre de recherche sur les risques et les crises

Source photo : LinkedIn
https://www.linkedin.com/posts/ms-erc_les-actes-dentreprendre-en-s%C3%A9curit%C3%A9-aes-activity-7072969912830312449-JylX?utm_source=share&utm_medium=member_desktop

Quelles sont les erreurs à éviter lors d'une cyberattaque ?

Interview

Nicolas-Loïc Fortin

Fondateur de polysécure et cofondateur du **salon de cybersécurité séQCure**

La cybersécurité est devenue un enjeu majeur dans notre monde de plus en plus connecté. Les cyberattaques sont devenues monnaie courante, touchant tant les grandes entreprises que les particuliers. Face à cette réalité, il est essentiel de comprendre les erreurs à éviter, les mesures de prévention à prendre et l'évolution constante des menaces.

Dans cette interview captivante, nous avons eu l'opportunité de discuter avec Nicolas Loïc Fortin, un expert en gestion de crise et en cybersécurité. Avec sa vaste expérience dans le domaine, Nicolas partage avec nous des conseils avisés pour faire face aux cyberattaques et se prémunir efficacement contre les menaces croissantes.

Interview par Alexandre Fournier

Expert en gestion et simulation de crise

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

Au fil de la conversation, Nicolas met en évidence l'importance de rester calme et rationnel lors d'une cyberattaque, de se préparer en amont pour limiter les dommages, et de prendre des mesures proactives pour renforcer la sécurité des entreprises et des particuliers. De plus, il aborde l'évolution constante des menaces et les moyens de s'y adapter.

Préparez-vous à plonger dans cette conversation enrichissante avec Nicolas Loïc Fortin et à acquérir des connaissances précieuses pour naviguer dans le monde complexe de la cybersécurité.

Q : Quelles sont les erreurs à éviter lors d'une cyberattaque pour les entreprises, les particuliers et toute personne pouvant être impliquée dans une cyberattaque ?

R : La première erreur à éviter est de paniquer. La panique peut nous amener à commettre de nombreuses erreurs et nous empêcher de prendre des décisions rationnelles. Il est donc crucial de rester calme et de réfléchir avec le recul nécessaire pour analyser les différents éléments associés à la crise et prendre des décisions basées sur la rationalité plutôt que sur l'émotion.

Ensuite, il est important de ne pas poser des gestes irréfléchis et de ne pas agir de manière impulsive. Par exemple, dans le cas des entreprises, il est primordial de conserver les preuves de l'attaque afin de les utiliser pour remonter jusqu'à la source et reconstruire les systèmes. Il ne faut donc pas se précipiter pour tout effacer ou tout débrancher.

De plus, il est essentiel de se préparer en amont pour faire face à une éventuelle cyberattaque. Cela nécessite une planification et une préparation adéquates, afin de pouvoir réagir de manière réfléchie et organisée en cas d'incident. Une entreprise ou un individu non préparé se retrouverait davantage enclin à la panique et à la prise de décisions irrationnelles.

> **“ La panique peut nous amener à commettre de nombreuses erreurs et nous empêcher de prendre des décisions rationnelles. ”**
>
> *Nicolas-Loïc Fortin*

Q : Que faut-il faire pour limiter les dommages lors d'une cyberattaque ?

R : Lors d'une cyberattaque, il est important de contenir et de limiter la propagation des dommages. Une métaphore utile est de considérer l'attaque comme de l'eau qui entre dans nos systèmes. Il faut donc prendre des mesures pour contenir cette eau et limiter les dommages associés.

Cela peut impliquer des décisions difficiles, comme la fermeture temporaire d'un système critique. Cependant, il est essentiel de prendre ces décisions de manière réfléchie et rationnelle, en évaluant attentivement la situation et le niveau de menace. Agir rapidement et efficacement est important, mais cela doit toujours être basé sur une analyse objective de la situation, afin de ne pas causer davantage de dommages.

En fin de compte, la gestion de crise et la gestion d'incidents nécessitent un équilibre entre la rapidité d'action et le maintien d'une approche réfléchie et rationnelle.

La prise de décisions émotionnelles peut être préjudiciable, tandis que la rationalité et la préparation préalable jouent un rôle clé dans la limitation des dommages et la résolution de la crise.

S'ABONNER ici

Écoutez l'interview complet de Nicolas-Loïc Fortin

Q : Comment une entreprise peut-elle se prémunir contre les cyberattaques ?

R : Pour se prémunir contre les cyberattaques, une entreprise doit adopter une approche proactive en matière de sécurité. Tout d'abord, il est important de comprendre les menaces auxquelles elle est confrontée. Beaucoup d'entreprises sous-estiment les risques ou pensent qu'elles sont trop petites pour être ciblées. Il est essentiel de prendre conscience que toutes les entreprises, quelle que soit leur taille, peuvent être des cibles potentielles.

Ensuite, il est crucial de mettre en place des mesures de sécurité appropriées. Cela inclut l'utilisation de technologies de sécurité telles que des pare-feux, des antivirus et des systèmes de détection des intrusions. De plus, il est essentiel de former les employés aux bonnes pratiques de sécurité, comme l'utilisation de mots de passe forts, la sensibilisation aux attaques par hameçonnage et la protection des informations sensibles.

Enfin, il est important de rester à jour sur les dernières tendances et les nouvelles techniques d'attaques. La cybersécurité est un domaine en constante évolution, et il est essentiel de rester informé des nouvelles menaces et des moyens de s'en prémunir.

Q : Comment peut-on se prémunir contre les nouvelles formes d'attaques qui apparaissent constamment ?

R : Les nouvelles formes d'attaques peuvent présenter des défis, mais il est possible de se prémunir contre elles en adoptant une approche proactive. Il est essentiel de collaborer avec des professionnels de la cybersécurité qui se tiennent constamment informés des évolutions du paysage des menaces.

De plus, plutôt que de se focaliser sur chaque nouvelle menace spécifique, il est recommandé de se concentrer sur les moyens utilisés par les attaquants. Les tactiques et les méthodes d'attaque peuvent varier, mais les objectifs et les motivations des attaquants restent généralement les mêmes.

En renforçant les mesures de sécurité existantes, en sensibilisant continuellement les employés et en mettant en œuvre de bonnes pratiques de cybersécurité, les entreprises peuvent améliorer leur posture de sécurité et se prémunir contre une grande variété de nouvelles formes d'attaques.

Conclusion

Cette interview avec Nicolas Loïc Fortin nous a permis d'obtenir un aperçu précieux de la cybersécurité et des mesures à prendre pour faire face aux cyberattaques. En évitant les erreurs courantes, en se préparant adéquatement et en restant informé des nouvelles menaces, nous pouvons renforcer notre posture de sécurité et protéger nos données et nos systèmes. La rationalité, la préparation et la collaboration avec des experts sont des éléments clés pour faire face à ces défis en constante évolution. Gardons à l'esprit les conseils de Nicolas Loïc Fortin pour naviguer en toute confiance dans ce monde numérique complexe et en constante évolution.

Interview par Alexandre Fournier

Podcast à écouter sur PolySécure

Podcast sur la gestion de crise

10 étapes clés pour mettre en place un plan de gestion de crise

Autopsie d'une crise : LastPass

Simulez en 3D votre prochaine cyberattaque!

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

Téléchargez gratuitement 5 idées de scénarios de gestion de crise

Nous offrons GRATUITEMENT 1h de simulation de crise.

Attention le nombre de places est limité!

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

Résilience : La clé de la prospérité dans un monde incertain

Depuis une vingtaine d'années, on entend parler de plus en plus de la Résilience organisationnelle.
La norme ISO 22316 :2017 la décrit comme étant la capacité d'une organisation à absorber et à s'adapter à un environnement changeant pour lui permettre d'atteindre ses objectifs, de survivre et de prospérer.

par Denis Goulet MBCI

Fondateur du groupe RESIX
Consultant / Formateur en
Système de Management de la Continuité d'Activité

Mais les organisations n'existent pas en vase clos. En fait, elles évoluent à l'intérieur de communautés (pays, villes, industries, etc.). De plus, elles requièrent l'apport et le support de personnes (travail manuel, créativité, leadership, etc.) sans lesquels les organisations ne peuvent fonctionner. On doit alors se demander s'il est possible qu'une organisation soit résiliente lorsqu'elle existe dans une communauté non résiliente ou quand elle est supportée par des personnes non résilientes ?

Dans cet article, nous allons explorer les différents types de résilience et comment ils peuvent être interconnectés. Nous verrons également l'importance croissante de la résilience afin d'assurer la prospérité dans un monde en constante évolution.

Un concept multidimensionnel

De l'opinion de plusieurs experts dans le domaine, la résilience organisationnelle doit s'appuyer sur d'autres formes de résilience afin de fonctionner pleinement. Selon eux, la résilience est un concept multidimensionnel qui se manifeste principalement sous trois formes – organisationnelle, communautaire et personnelle.

Ces trois formes, bien que distinctes, sont profondément interconnectées et se renforcent mutuellement, créant un écosystème qui permet à une organisation non seulement de survivre à une perturbation, mais aussi de prospérer face aux défis qu'elle rencontre.

La résilience organisationnelle

La résilience organisationnelle permet à une organisation d'anticiper et de répondre aux menaces et aux opportunités provenant de changements soudains ou progressifs, dont l'origine est interne ou externe. Ainsi, elle contribue à l'atteinte des objectifs stratégiques, de survivre et même de prospérer, quoi qu'il arrive.

Ce type de résilience résulte de bonnes pratiques commerciales et d'une gestion efficace. Cela peut impliquer plusieurs éléments dont des stratégies de gestion des risques, des plans de continuité, la cybersécurité, des systèmes robustes et flexibles, le respect des lois et une culture organisationnelle qui valorise et favorise la résilience. L'amélioration de la résilience organisationnelle peut même devenir un objectif organisationnel stratégique en soi.

On pourrait penser que l'atteinte d'une résilience organisationnelle dépendrait largement de décisions internes à l'organisation. Cependant, nous croyons que la résilience organisationnelle ne peut être atteinte quand l'organisation œuvre dans un environnement communautaire qui n'est pas résilient. On peut penser à une usine construite près d'une rivière dont la digue est mal entretenue par la ville.

De même, lorsque les individus au sein de l'organisation ne sont pas résilients, ils auront de la difficulté de contribuer à son succès. On peut penser à des employés dont le salaire leur permet difficilement de faire face au coût de la vie dans un contexte d'inflation.

La version anglaise de cet article a été publiée dans

The Resilience Post

Une organisation peut avoir des plans de continuité d'activité robustes, mais si une catastrophe naturelle frappe la communauté et détruit les infrastructures locales, l'organisation sera inévitablement touchée.

La résilience communautaire

La résilience communautaire est la capacité d'une communauté à se préparer, à répondre, à s'adapter et à se remettre des perturbations. Cela peut impliquer plusieurs éléments dont des infrastructures robustes et bien entretenues, des systèmes de soutien social, des plans d'urgence communautaires et une culture de résilience.

Une organisation peut avoir des plans de continuité d'activité robustes, mais si une catastrophe naturelle frappe la communauté et détruit les infrastructures locales, l'organisation sera inévitablement touchée. On peut penser à des inondations, des pannes d'électricité majeures, des feux de forêt, etc.

L'organisation peut contribuer à la résilience communautaire en s'impliquant dans les programmes d'amélioration de la communauté par des subventions, des dons d'équipement, des collectes de fonds, des journées bénévoles, etc., ou lors de la réponse à des événements en mettant à la disposition de la communauté des ressources (de l'équipement, des véhicules, des locaux, de la nourriture, des biens essentiels, etc.).

Il pourrait alors se créer une meilleure compréhension des besoins mutuels et une meilleure coopération qui aurait pour effet d'augmenter la résilience communautaire dans laquelle se trouve l'organisation et, conséquemment, augmenter la résilience de l'organisation.

La résilience personnelle

La résilience personnelle fait référence à la capacité d'un individu à faire face, à s'adapter et à se remettre des défis et des adversités qu'il rencontre dans sa vie. Cela peut impliquer des compétences de gestion du stress, une attitude positive, la capacité à résoudre les problèmes et à prendre des décisions, et un réseau de soutien solide.

L'organisation peut contribuer à la résilience personnelle en adoptant une culture respectueuse de l'employé (équilibre travail-famille, horaire de travail adapté, salaire suffisant, programmes d'avantages sociaux, etc.) et un environnement de travail sécuritaire, tant au niveau physique que psychologique. Des employés en bonne santé et heureux peuvent mieux se concentrer sur leur travail. Cela a un impact direct sur la qualité, la satisfaction des clients et la rentabilité.

Des employés résilients sont donc essentiels pour une organisation résiliente, car ce sont eux qui mettent en œuvre les stratégies afin d'atteindre les objectifs de l'organisation, qui adaptent leur façon de travailler face aux changements et qui continuent à fonctionner efficacement en période de stress ou de perturbation.

De la continuité d'activité à la résilience

Pour beaucoup, les concepts de résilience ne sont pas encore clairs. La résilience est souvent perçue comme une dépense optionnelle pour se prémunir contre les perturbations.

Plus simplement, on peut voir la résilience comme une espèce d'évolution de la continuité d'activité. Ainsi, la continuité d'activité concerne la capacité d'une organisation à maintenir ses opérations essentielles pendant et après une perturbation.

Cela implique d'avoir des plans et des systèmes en place pour gérer les crises et s'en remettre rapidement. Avec la continuité d'activité, les organisations peuvent réduire de beaucoup les coûts associés aux interruptions d'activité, comme la perte de revenus, les pénalités contractuelles et la perte de confiance des clients.

La résilience, quant à elle, va au-delà de la simple reprise après une perturbation.

Elle concerne la capacité d'une organisation à s'adapter et à prospérer face au changement et à l'incertitude. Cela implique d'avoir une culture, des systèmes et des processus flexibles qui permettent à l'organisation d'évoluer. En investissant dans la résilience, les organisations peuvent non seulement survivre aux défis, mais aussi saisir de nouvelles opportunités et innover.

L'avenir de la résilience

En regardant vers l'avenir, on peut penser que la résilience va se développer et devenir une compétence indispensable pour assurer la pérennité et la réussite de toutes les organisations. À l'instar de la continuité d'activité qui est devenue une exigence standard dans le monde des affaires, la résilience suivra tout probablement le même chemin.

Dans un monde de plus en plus complexe et incertain, la capacité à s'adapter et à prospérer face au changement et à l'adversité est essentielle. Les organisations qui sont capables de faire preuve de résilience seront mieux placées pour gérer les défis et saisir les opportunités qui se présentent.

Dans un avenir rapproché, on peut s'attendre à ce que les organisations demandent à leurs fournisseurs de démontrer leur résilience, tout comme elles demandent aujourd'hui à voir leurs capacités de continuité d'activité et de protection des données. La résilience ne sera pas seulement un avantage concurrentiel, mais une exigence.

L'avènement du « Chief Resilience Officer »

Mais qui est le Chef d'orchestre qui pourra mettre en place et entretenir la résilience d'une organisation ?

Depuis quelques années, un nouveau poste se dessine dans les organisations; le « Chief Resilience Officer » (CRO). Le titre est utilisé dans le cadre de l'initiative « 100 Resilient Cities », parrainée par la Fondation Rockefeller.

Ce poste couvre les aspects de risques, sécurité, continuité, mesures d'urgence, chaîne d'approvisionnement, gestion de crise, gouvernance, santé & sécurité, et plusieurs autres (voir Annexe A de la norme ISO 22316 :2017).

Cette personne est un membre essentiel de l'équipe de Direction et prend part aux décisions stratégiques de l'organisation afin d'instaurer et de maintenir la résilience au sein d'une organisation. Le/la CRO coordonne les initiatives de résilience, prépare l'organisation à diverses perturbations et collabore avec tous les départements pour intégrer la résilience dans les pratiques commerciales.

Le/la CRO promeut une culture de résilience personnelle, s'assurant que les employés sont formés à la gestion du stress et renforçant les réseaux de soutien internes. Il/elle travaille également avec la communauté locale pour soutenir la résilience communautaire, contribuant à des projets d'infrastructure et soutenant les initiatives locales.

De plus en plus d'organisations mettent en place un poste de « Chief Resilience Officer », tels qu'en témoignent cet article dans Forbes et les offres d'emploi dans LinkedIn.

En intégrant la résilience dans tous les aspects de l'organisation, le/la CRO transforme les crises en opportunités, assurant la prospérité de l'organisation dans un monde en constante évolution.

Cela signifie que les organisations devront intégrer la résilience dans tous les aspects de leur fonctionnement. Cela va au-delà de la simple mise en place de plans de continuité d'activité ou de gestion des risques. Cela implique de créer une culture de résilience, de développer des systèmes et des processus flexibles, et de renforcer la résilience personnelle et communautaire.

La résilience se révèle être un concept essentiel dans un monde en perpétuel mouvement. En intégrant les trois facettes de la résilience - organisationnelle, personnelle et communautaire - les individus, les organisations et les communautés peuvent non seulement survivre aux défis et aux perturbations d'un monde incertain, mais aussi prospérer.

Article écrit par Denis Goulet, MBCI

La version anglaise de cet article a été publiée dans [The Resilience Post]

Denis Goulet, MBCI est un expert reconnu dans le domaine des systèmes de gestion de la continuité des activités (SGCA) avec plus de 31 ans d'expérience couvrant les organisations financières, de télécommunications, pharmaceutiques, industrielles, manufacturières, de distribution et gouvernementales. Au fil des ans, Denis a accompagné ces organisations dans la définition, le développement, la mise en place, la maintenance et l'exercice de leur SMCA. Depuis 1999, Denis a développé une carrière internationale où il fournit des services de conseil et de coaching BCMS ainsi que des formations BCMS de haute qualité aux professionnels BCMS d'organisations privées et publiques, en Amérique du Nord, en Europe, en Afrique et au Moyen-Orient. En 1992, Denis obtient la certification CBCP (DRI International). Il a également obtenu en 2008 la certification MBCI (Business Continuity Institute). En 2012, il est devenu Lead Implementer certifié ISO 22301 et Lead Auditor certifié ISO 22301 (PECB). Denis a contribué à la communauté BCM en tant que membre du conseil d'administration de « DRIE-Montréal » (1999-2000) et de « Disaster Recovery Institute Canada » (1998-2000). Il siège au BC Management International Benchmarking Advisory Board depuis 2008 et a été le leader fondateur du forum BCI-Québec (2009-2010). Denis a fondé BCMIX en 2007 et gère cette communauté internationale virtuelle de Business Continuity Management qui compte plus de 14 000 membres. Denis a reçu un BCI Achievement Award en 2012 pour avoir dirigé le groupe LinkedIn le plus performant lié à la continuité des activités. Conférencier expérimenté et enthousiaste depuis 1994, Denis est intervenu sur divers sujets comme ISO22301, exercices BCM, Business Impact Analysis (BIA), vente de BCM à la haute direction, etc. , représentant d'entreprise, managers, cadres, etc.) dans les secteurs privé et public. Denis parle couramment l'anglais et le français.

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

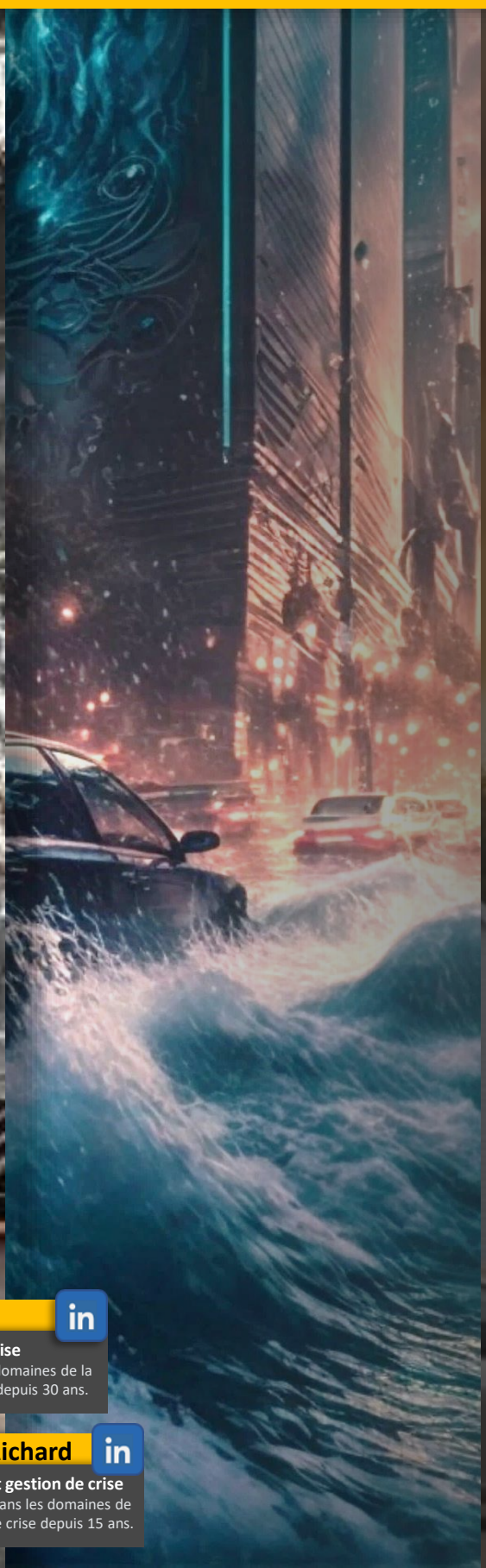
Profitez de vos vacances pour lire

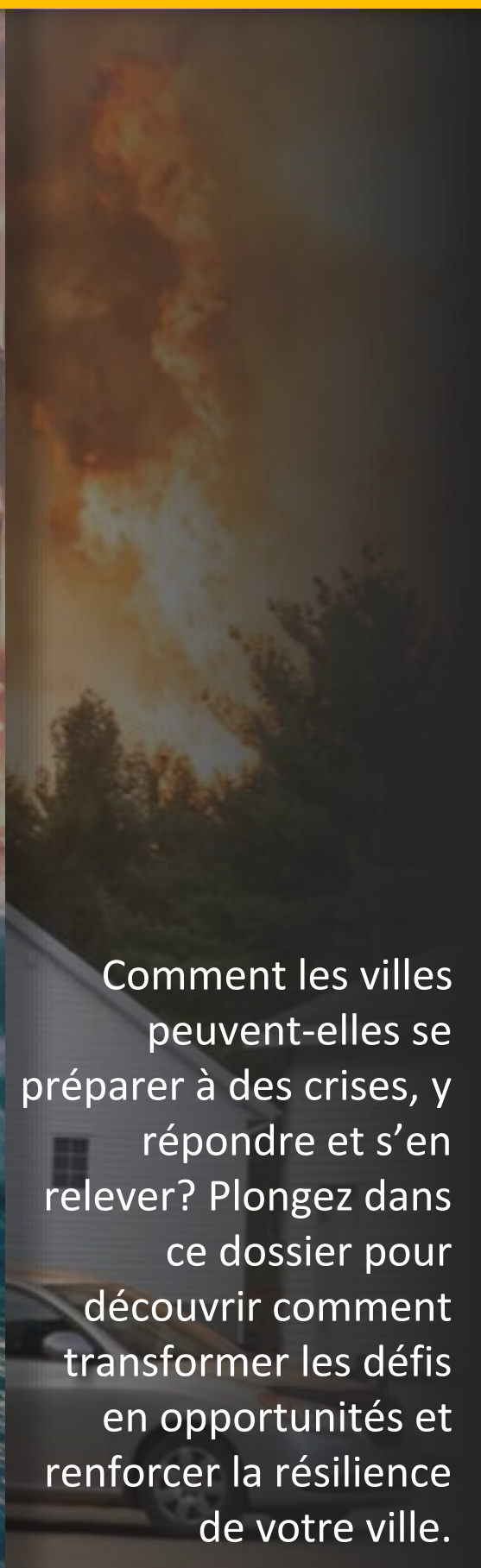
Lire ce magazine

Profitez de vos vacances pour lire

Lire ce magazine

Gestion de la continuité des services dans les villes





Comment les villes peuvent-elles se préparer à des crises, y répondre et s'en relever? Plongez dans ce dossier pour découvrir comment transformer les défis en opportunités et renforcer la résilience de votre ville.

par Alexandre Fournier

Expert en gestion et simulation de crise

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

Par Karine Maréchal-Richard

Experte en continuité des affaires et gestion de crise

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

Pour des questions de facilités de lecture, nous avons regroupé les intitulés « commune », « municipalité », « agglomération » sous l'intitulé « ville »…

Que vous soyez maire, membre du personnel d'une mairie, d'une ville, ou simplement un citoyen concerné par la résilience de votre ville, cet article est pour vous. Dans un monde où les défis imprévus sont devenus la norme plutôt que l'exception, la capacité à maintenir la continuité des services essentiels en temps de crise est devenue une compétence cruciale pour toute collectivité.

Des catastrophes naturelles aux crises sanitaires, en passant par les incidents technologiques, les crises sociales ou émeute comme celle de France de juin 2023, les services offerts par les villes, que nous tenons pour acquis peuvent être perturbés, voire complètement interrompus, en un instant.

Les services tels que l'eau potable, l'électricité, l'éducation, la sécurité publique et les transports sont le cœur battant de nos villes. Leur indisponibilité, même temporaire, peut avoir des conséquences dévastatrices.

C'est pourquoi la préparation aux crises revêt une importance capitale pour les maires, les élus et les gestionnaires, car elles deviennent de plus en plus nombreuses, multiformes et imprévisibles. Il est important d'anticiper l'imprévisibilité des crises et de développer des scénarios d'approche proactive et adaptée à de telles situations. Cela implique alors pour les villes d'élaborer différents plans qui leur permettront :

- De maintenir les services municipaux essentiels pour répondre aux besoins de la population à l'aide d'un plan de continuité des activités (PCA);
- D'établir des mécanismes de prévention pour anticiper les risques, pour diffuser l'information et pour assurer l'alerte de la population, tout en garantissant la protection des individus, des biens et de l'environnement contre les crises. Ce plan est connu sous le nom de plan de sécurité civile municipale au Québec et est appelé en France, plan communal de sauvegarde (PCS);
- De définir une stratégie de communication qui détaille les mesures à prendre pour garantir une communication efficace avec toutes les parties prenantes de la ville telles que la population, les autorités, les entreprises privées et publiques, etc. Ainsi, cela permettra de protéger la réputation, l'image et la confiance des parties prenantes d'une administration municipale ou communale.

Dans ce dossier, nous allons explorer les différentes causes potentielles d'indisponibilité des services et discuter des stratégies de prévention et de mitigation.

Nous aborderons également des sujets tels que la gestion de la communication en temps de crise, la gestion des ressources humaines, l'évaluation et l'amélioration continue, et bien plus encore.

Que vous soyez un professionnel de la gestion de crise ou un citoyen souhaitant comprendre comment votre ville se prépare aux défis à venir, nous espérons que vous trouverez cet article utile et instructif.

Comprendre les risques

Dans un monde en constante évolution, comprendre les risques est la première étape pour assurer la résilience des villes. Cette section explore les différentes causes potentielles d'indisponibilité des services et illustre, à travers des études de cas, comment différentes crises peuvent impacter les services municipaux.

Les causes potentielles d'indisponibilité des services

Les causes potentielles d'indisponibilité des services peuvent être nombreuses et variées. Elles peuvent être largement catégorisées en catastrophes naturelles, en défaillances technologiques ou d'infrastructure, et en accidents induits par l'homme.

- **Catastrophes naturelles :** Cela comprend des événements tels que les tremblements de terre, les inondations, les ouragans, les tornades, les incendies de forêt et les pandémies. Ces événements peuvent causer des perturbations et des dommages généralisés aux services municipaux.
- **Défaillances technologiques ou d'infrastructures :** Cela regroupe des événements tels que les pannes de courant, les cyberattaques, la contamination de l'approvisionnement en eau, les pannes de télécommunications ou les défaillances d'autres infrastructures critiques. Ces défaillances peuvent perturber les services essentiels, entraînant ainsi des conséquences directes sur la vie quotidienne des citoyens.
- **Événements induits par l'homme :** Cela inclut des événements tels que le terrorisme, les troubles civils ou d'autres formes de perturbations intentionnelles. Ces accidents peuvent provoquer des interruptions significatives des services, menaçant ainsi la sécurité publique et nécessitant une réponse rapide et coordonnée de la part des autorités municipales ou communales.

PHOTO : Émeute France 2023 – Twitter

Exemples de crises et de leurs impacts sur les services municipaux

Les exemples ci-dessous illustrent les impacts de divers types de crises sur les services municipaux et communaux. Ils soulignent l'importance d'une planification d'urgence robuste et de mesures de préparation pour assurer la continuité des services essentiels et protéger la population pendant une crise ou une catastrophe.

- **Catastrophe de l'usine Lubrizol à Rouen, France (2019)** : L'incendie de l'usine Lubrizol à Rouen, survenu le 26 septembre 2019, a engendré d'importantes inquiétudes sanitaires et environnementales. Cet accident dans une usine de produits chimiques classée *Seveso a produit un large panache de fumée et a impacté économiquement la région. Malgré l'absence de victimes, des questions demeurent concernant la présence de produits dangereux à la suite de l'incendie.
- **Pandémie de COVID-19 (2019-présent)** : La pandémie de COVID-19 en cours a fortement sollicité les systèmes de santé du monde entier et a perturbé de nombreux autres services municipaux. De nombreuses villes ont dû s'adapter rapidement à l'évolution des circonstances, mettant en œuvre de nouvelles mesures telles que des politiques de travail à distance, des directives de distanciation sociale et des protocoles sanitaires renforcés.
- **Cyberattaque de la Ville de Lille, France (2023)**: Cette cyberattaque a eu d'importants impacts sur les services offerts par la Ville de Lille. De nombreux systèmes informatiques de la Ville ont été mis hors ligne, ce qui a affecté le fonctionnement des services municipaux. La plateforme téléphonique de la Ville était inaccessible jusqu'à nouvel ordre et la gestion et la délivrance d'actes d'état civil a fonctionné de façon manuscrite. La plupart des services publics ont été perturbés, puisque leur fonctionnement dépend le plus souvent d'une infrastructure informatisée. Pour éviter que le problème se propage, la ville explique avoir interrompu le système informatique et avoir demandé aux élus et aux agents municipaux de ne pas rallumer leurs ordinateurs. Cela a conduit à une perturbation majeure dans tous les services municipaux.
- **Catastrophe due aux feux de forêt au Québec, (2023-présent)** : En raison de nombreux incendies très actifs en Abitibi et dans le Nord-du-Québec, des Villes comme Chibougamau et Lebel-sur-Quévillon ont été obligées d'évacuer leur population et de transférer leurs services essentiels vers d'autres villes. Certaines routes ont été bloqués à cause des incendies et la qualité de l'air inquiète au-delà des zones évacuées. Toute l'économie locale est à l'arrêt : pourvoirie, tourisme, industrie forestière et minière sont en suspens, en plus de tous les bâtiments et les équipements détruits ou ravagés par les flammes.

Les sites Seveso produisent ou stockent des substances pouvant être dangereuses pour l'homme et l'environnement)

Préparation et planification

La préparation et la planification sont des éléments essentiels pour assurer la continuité des services et la protection de la population en cas de crise. Elles permettent de prévenir et de mitiger les impacts potentiels d'une crise, de former et de sensibiliser la population, et de mettre en place des systèmes de secours et de redondance informatique ou autre.

- **Prévention et mitigation immédiate**

  La prévention est la première étape pour assurer la continuité des services et la protection de la population. Elle consiste à identifier les risques potentiels et à mettre en place des mesures pour les atténuer. Par exemple, cela peut impliquer l'application de protocoles pour gérer les situations d'urgence, comme indiqué dans le Plan de sécurité civile de la Ville de Québec.

  En cas de situation d'urgence, des mesures d'intervention immédiate sont nécessaires pour préserver la vie, protéger les personnes, assurer leurs besoins essentiels et sauvegarder les biens ainsi que l'environnement. Ces mesures peuvent inclure des actions de sauvetage, ainsi que la sécurisation et la restauration de sites.

- **Formation et sensibilisation du personnel municipal et de la population**

  La formation et la sensibilisation du personnel municipal (communal) et de la population sont également cruciales pour assurer une réponse efficace en cas de crise. Cela peut inclure des formations sur les protocoles d'urgence, des exercices de simulation de crise et des activités de sensibilisation pour aider le personnel municipal et la population à comprendre les risques et les mesures à prendre en cas de crise.

- **Mise en place de systèmes de secours et de redondance**

  Enfin, la mise en place de systèmes de secours et de redondance informatique est une autre étape clé de la préparation et de la planification. Ces systèmes permettent de garantir la continuité des services en cas de défaillance des logiciels et des équipements principaux. Cela peut inclure la mise en place de systèmes de communication de secours, de gestion des ressources humaines et matérielles ainsi que de plans de continuité des services en cas de crise.

Mise en place des différents plans pour gérer une crise

Confrontées à une multitude de défis, les villes doivent mettre en place des plans solides pour gérer efficacement les crises.

La création d'un Plan Communal de Sauvegarde (PCS) ou d'un plan de sécurité civile municipale, l'établissement d'un Plan de continuité des activités (PCA), ainsi que le développement d'un Plan de communication de crise sont des étapes clés dans cette démarche stratégique.

Ces plans constituent une fondation solide pour anticiper, préparer, répondre et se rétablir en cas de crises.

Plan Communal de Sauvegarde (PCS) ou un Plan de Sécurité Civile Municipale (PSCM)

La mise en place d'un PCS ou d'un plan de sécurité civile municipale est une démarche essentielle pour les villes. Ce plan stratégique permet de prévoir et de gérer efficacement les situations d'urgence, en mobilisant les ressources et les acteurs nécessaires.

Ce plan est un outil de gestion de crise conçu pour assurer la sécurité de la population en cas de risques majeurs. Il vise à prévoir les actions à mener et les moyens à utiliser pour assurer la protection des personnes, des biens et de l'environnement.

Le PCS ou PSCM est un document opérationnel qui définit l'organisation prévue par la ville, pour assurer l'alerte, l'information, la protection et le soutien de la population en cas d'événement exceptionnel.

> “ Une bonne préparation est la clé du succès. ”
>
> *Alexander Graham Bell*

Plan de continuité des activités (PCA)

L'élaboration d'un PCA est une autre démarche essentielle pour continuer à honorer sa mission en cas de sinistre.

Ce plan permet de définir à l'avance qui fait quoi, comment et avec qui pour maintenir les activités essentielles des villes et il fait partie du plan de gestion de crise.

Le PCA guide les responsables des activités essentielles sur les actions à réaliser en cas d'indisponibilité de leur environnement de travail ou d'une défaillance informatique telle qu'une cyberattaque, indisponibilité d'un fournisseur infonuagique, destruction de son centre informatique, etc.

Pour être efficace en période de crise, le PCA doit être pratico-pratique et connu par toutes les personnes clés.

Plan de communication de crise

La gestion de la communication est un pilier fondamental de la gestion de crise. Une communication transparente et régulière joue un rôle crucial pour maintenir la confiance du public, diffuser des informations essentielles et coordonner efficacement les efforts de réponse.

Cependant, il est tout aussi important de centraliser la communication et de personnaliser les messages en fonction des destinataires.

Principales étapes pour établir un PCA, un PCS ou un plan de sécurité civile municipale :

- Nommer un responsable.
- Réaliser un état de situation sur la documentation existante.
- Réaliser un plan d'action sur ce qui doit mis en place pour atteindre les objectifs de continuité des activités et de protection de la population.
- Identifier et évaluer les risques auxquels la ville est exposée.
- Définir les actions à mener pour prévenir ou limiter les conséquences de ces risques ainsi que l'organisation des moyens nécessaires pour mettre en œuvre ces actions
- Documenter tous les plans depuis l'alerte jusqu'à la résolution de la crise.
- Former et sensibiliser la population et les acteurs clés impliqués dans le PCA.
- Réaliser des exercices et des tests avec la population et les acteurs clés du PCA.
- Actualiser les plans afin qu'ils soient toujours opérationnels.

Prévention - Préparation - Intervention - Rétablissement

Engagement communautaire

L'engagement de la communauté est non seulement essentiel, mais souvent indispensable dans la préparation et la réponse aux crises. Les villes, malgré leur volonté, sont souvent limitées en termes de ressources humaines et ne peuvent pas toujours répondre de manière autonome à toutes les situations d'urgence. Dans ce contexte, les citoyens, en tant que premiers témoins et potentiels premiers intervenants lors d'une crise, deviennent une ressource précieuse.

Leur participation active peut jouer un rôle crucial dans la minimisation des impacts d'une crise et dans la récupération post-crise. L'implication de la communauté permet ainsi de compléter et d'amplifier les efforts de la ville, renforçant ainsi la résilience de l'ensemble de la collectivité.

Importance de l'engagement de la communauté dans la préparation

L'engagement précoce et continu de la communauté dans la préparation aux crises est d'une importance capitale. En intégrant les citoyens dès les premières étapes de la planification, on peut non seulement sensibiliser ces derniers aux risques potentiels, mais aussi développer leurs connaissances et leurs compétences nécessaires pour réagir efficacement.

Cette approche proactive peut renforcer considérablement la résilience de la communauté, car les citoyens bien informés et préparés sont plus susceptibles de se remettre rapidement d'une crise.

De plus, l'implication des citoyens dès le début du processus de planification de la continuité et de la réponse aux crises peut s'avérer inestimable.

Les citoyens, en tant que résidents et utilisateurs des services locaux, peuvent fournir des informations locales précieuses, aider à identifier les vulnérabilités et les ressources de la communauté, et proposer des solutions innovantes pour gérer les risques.

Stratégies pour impliquer les citoyens dans les plans de gestion de crise

Il existe plusieurs stratégies pour impliquer les citoyens dans les plans de gestion de crise :

- **Éducation et sensibilisation :** Il est essentiel d'informer les citoyens sur les risques potentiels et de leur fournir des informations sur la manière de se préparer et de réagir. Cela peut être fait par le biais de campagnes de sensibilisation, de formations, de simulations de crise et par la diffusion d'informations via des canaux de communication accessibles (affiches, dépliants, vidéos, site internet de la ville, etc.).
- **Participation à la planification :** Les citoyens peuvent être invités à participer à la planification de la continuité et de la réponse aux crises. Cela peut impliquer des consultations publiques, des ateliers de planification participative et l'inclusion de représentants de la communauté dans les comités de planification.
- **Volontariat :** Les citoyens peuvent être encouragés à s'impliquer directement dans la réponse aux crises en devenant des volontaires. Cela peut impliquer la formation de groupes de volontaires pour aider à des tâches précises lors d'une crise, comme la distribution de fournitures, l'aide aux évacuations ou le soutien aux personnes vulnérables.
- **Retour d'expérience et évaluation :** Après une crise, il est important de recueillir les commentaires des citoyens sur la réponse à la crise et d'utiliser ces informations pour améliorer les plans de continuité et de réponse aux crises.

L'engagement de la communauté n'est pas seulement une stratégie gagnant-gagnant, mais un élément vital et déterminant pour la réussite d'une gestion de crise municipale ou communale. En renforçant la résilience de la communauté, cela, contribue directement à la qualité et à l'efficacité des plans de continuité et de réponse aux crises. L'implication de la communauté est donc un facteur clé, voire indispensable, pour assurer une gestion de crise efficace et résiliente.

Coopération intercommunale et intermunicipale

La coopération intercommunale ou intermunicipale, bien que souvent négligée, est un aspect crucial de la préparation et de la réponse aux crises. Les crises ne connaissent pas de frontières administratives et peuvent souvent affecter plusieurs villes à la fois.

De plus, toutes les villes ne disposent pas des mêmes ressources et capacités pour faire face aux crises. Certaines peuvent avoir plus de moyens financiers, de personnel ou d'équipements que d'autres. Dans ce contexte, la coopération et la solidarité intercommunale deviennent non seulement bénéfiques, mais souvent indispensables pour une gestion efficace des crises.

Importance de la coopération avec d'autres villes

La coopération intercommunale ou intermunicipale peut prendre de nombreuses formes, allant du partage d'informations et de ressources à la coordination des réponses en cas de crise.

En travaillant ensemble, les villes peuvent tirer parti de leurs ressources collectives, partager les meilleures pratiques et apprendre les unes des autres. Cela peut également aider à assurer une réponse plus cohérente et coordonnée en cas de crise, ce qui peut réduire les impacts et accélérer la récupération.

Exemple de coopération réussie et de leçons apprises

Il existe de nombreux exemples de coopération intercommunale ou intermunicipale réussie. Par exemple, lors de catastrophes naturelles majeures comme des inondations ou des tremblements de terre, plusieurs villes ont travaillé ensemble pour coordonner leurs efforts de secours et de récupération. Elles ont partagé des informations en temps réel, coordonné l'évacuation des résidents et ont partagé des ressources, comme des équipements d'urgence et des fournitures de secours.

Cet exemple montre que la coopération peut être un outil puissant pour gérer les crises. Cependant, pour que cette collaboration soit efficace, il est important de mettre en place des mécanismes de coopération avant qu'une crise se produise. Cela peut inclure la création de forums de coopération intercommunale, la mise en place de protocoles de partage d'informations et la formation conjointe des personnels de secours.

Rôle des partenaires externes

Dans la gestion de crises, les partenaires externes, qu'ils soient locaux ou plus éloignés, jouent un rôle crucial. Ces partenaires peuvent inclure des entreprises de services publics, des organisations non gouvernementales, des agences gouvernementales et d'autres entités qui peuvent apporter une aide précieuse lors d'une crise.

Les acteurs locaux, avec leur connaissance approfondie de la communauté, de ses ressources et de ses défis, ainsi que leur proximité géographique, peuvent souvent agir plus rapidement et de manière plus ciblée, en tenant compte des particularités et des besoins de la communauté locale.

Cependant, les partenaires plus éloignés ont également un rôle important à jouer. Par exemple, les agences gouvernementales nationales ou régionales peuvent fournir des ressources et des compétences spécialisées qui ne sont pas disponibles localement. De même, les organisations non gouvernementales nationales ou internationales peuvent apporter une expertise et une capacité d'intervention supplémentaires, en particulier dans les situations de crise majeure.

Discussion sur le rôle des partenaires externes

Les partenaires externes, avec leur variété de ressources et de compétences, sont des acteurs essentiels dans la gestion des crises. Leur intégration en amont, lors de la phase de préparation, est cruciale pour une gestion efficace des crises.

Les entreprises de services publics, lorsqu'elles sont impliquées dès le début, peuvent collaborer à l'élaboration de scénarios d'intervention, déterminer les moyens à engager en fonction de l'événement et planifier des mesures pour rétablir rapidement les services essentiels tels que l'électricité, l'eau et les communications après une crise.

Les entreprises privées, telles que les entreprises d'excavation, de construction et autres, peuvent également jouer un rôle crucial. Leur expertise technique et leur capacité à mobiliser rapidement des ressources matérielles peuvent être inestimables pour la réparation et la remise en état des infrastructures endommagées.

Les organisations non gouvernementales telles que la Croix-Rouge et autres associations locales, lorsqu'elles sont intégrées dans la planification, peuvent préparer des plans d'aide humanitaire, comme la distribution de nourriture, d'eau, d'abris et de soins médicaux. Leur participation active dans la préparation permet de définir clairement leurs rôles et leurs responsabilités en fonction des différents scénarios de crise envisagés.

Les agences gouvernementales, lorsqu'elles sont engagées tôt, peuvent fournir un soutien en termes de coordination, de financement et de ressources spécialisées. Leur implication dès le début permet d'aligner les plans de gestion de crise de la ville avec les plans régionaux ou nationaux, et de s'assurer que les ressources nécessaires seront disponibles en cas de crise.

L'intégration en amont de ces partenaires externes dans la planification de la gestion des crises, en fonction des scénarios d'intervention, permet non seulement de déterminer les moyens à engager et la répartition des rôles de chacun, mais aussi d'améliorer grandement la capacité d'une ville à répondre efficacement lorsqu'une crise survient.

Comment établir et maintenir des relations efficaces avec les partenaires

Établir des relations avec les partenaires externes est une première étape cruciale, mais il est tout aussi important de maintenir ces relations au fil du temps. Cela nécessite une communication ouverte et régulière, une coordination étroite et une compréhension mutuelle des rôles et des responsabilités.

Voici quelques stratégies pour y parvenir :

- **Communication régulière :** Il est important de maintenir une communication en continu avec les partenaires, même en dehors des périodes de crise. Cela peut aider à construire la confiance, à résoudre les problèmes avant qu'ils ne deviennent des crises et à s'assurer que tout le monde est sur la même longueur d'onde en ce qui concerne les plans et les procédures de gestion de crises.
- **Simulations et exercices conjoints :** Les simulations et exercices conjoints peuvent aider à tester les plans de gestion de crises, à identifier les lacunes et les points d'amélioration, et à renforcer la coordination et la coopération entre les partenaires.
- **Accords formels :** Les accords formels, tels que les protocoles d'entente ou les accords de niveau de service, peuvent aider à clarifier les rôles et les responsabilités de chaque partenaire et à établir des procédures pour la coordination et la communication pendant une crise.
- **Formation et éducation :** La formation et l'éducation peuvent aider à assurer que tous les partenaires comprennent les risques potentiels, les plans de gestion de crises, leurs responsabilités et leurs rôles respectifs.

Gestion des ressources humaines en temps de crise

La gestion des ressources humaines est un aspect crucial et incontournable de la réponse aux crises. Les personnes qui se trouvent sur le terrain sont en première ligne lors d'une crise, et leur rôle est essentiel pour assurer le bon fonctionnement de la réponse. Leur bien-être, leur résilience et leurs compétences sont des facteurs déterminants qui influencent grandement l'efficacité de la réponse à la crise.

Sans ces acteurs clés, rien ne fonctionne de manière optimale. Ils sont les véritables héros qui font face aux défis, prennent des décisions rapides et mettent en œuvre des actions concrètes pour atténuer les effets de la crise. Leur dévouement, leur courage et leur expertise sont indispensables pour protéger les vies, maintenir les services essentiels et contribuer à la reprise après la crise.

Il est donc impératif de veiller au bien-être de ces professionnels sur le terrain, en leur offrant un soutien adéquat et en reconnaissant l'importance cruciale de leur travail. Cela comprend la gestion du stress, le soutien psychologique, l'accès à des ressources en santé mentale, ainsi que des mesures visant à préserver leur sécurité et leur santé physique.

La réussite de la gestion de crises repose en grande partie sur ces personnes dévouées qui se trouvent sur le terrain. Leur engagement et leur expertise sont indispensables pour assurer une réponse efficace et protéger la communauté lors des moments les plus difficiles. Leur contribution inestimable mérite d'être reconnue et soutenue tout au long du processus de gestion de crises.

Il est également essentiel d'investir, avant la crise, dans leur développement professionnel et de renforcer leurs compétences en matière de gestion de crise. Des formations régulières, des exercices de simulation et des opportunités d'apprentissage en continu sont nécessaires pour les préparer à faire face à différents scénarios de crise, à prendre des décisions éclairées et à travailler de manière coordonnée avec d'autres acteurs.

La gestion des ressources humaines est un aspect crucial et incontournable de la réponse aux crises. Les personnes qui se trouvent sur le terrain sont en première ligne lors d'une crise, et leur rôle est essentiel pour assurer le bon fonctionnement de la réponse. Leur bien-être, leur résilience et leurs compétences sont des facteurs déterminants qui influencent grandement l'efficacité de la réponse à la crise.

Législation et réglementation

La législation et la réglementation jouent un rôle fondamental dans la gestion de crises et la continuité des services.

Elles établissent les cadres juridiques et les exigences auxquelles les villes doivent se conformer pour assurer une gestion efficace des crises.

Présentation des lois et des règlements pertinents

Il existe une variété de lois et de règlements qui sont précisément conçus pour encadrer la gestion de crise et la continuité des services au niveau communal ou municipal.

Ces textes législatifs peuvent traiter de divers aspects tels que la préparation aux crises, les plans d'urgence, la coordination des acteurs, la protection des populations, la protection des infrastructures critiques, la communication en temps de crise, et bien d'autres sujets connexes.

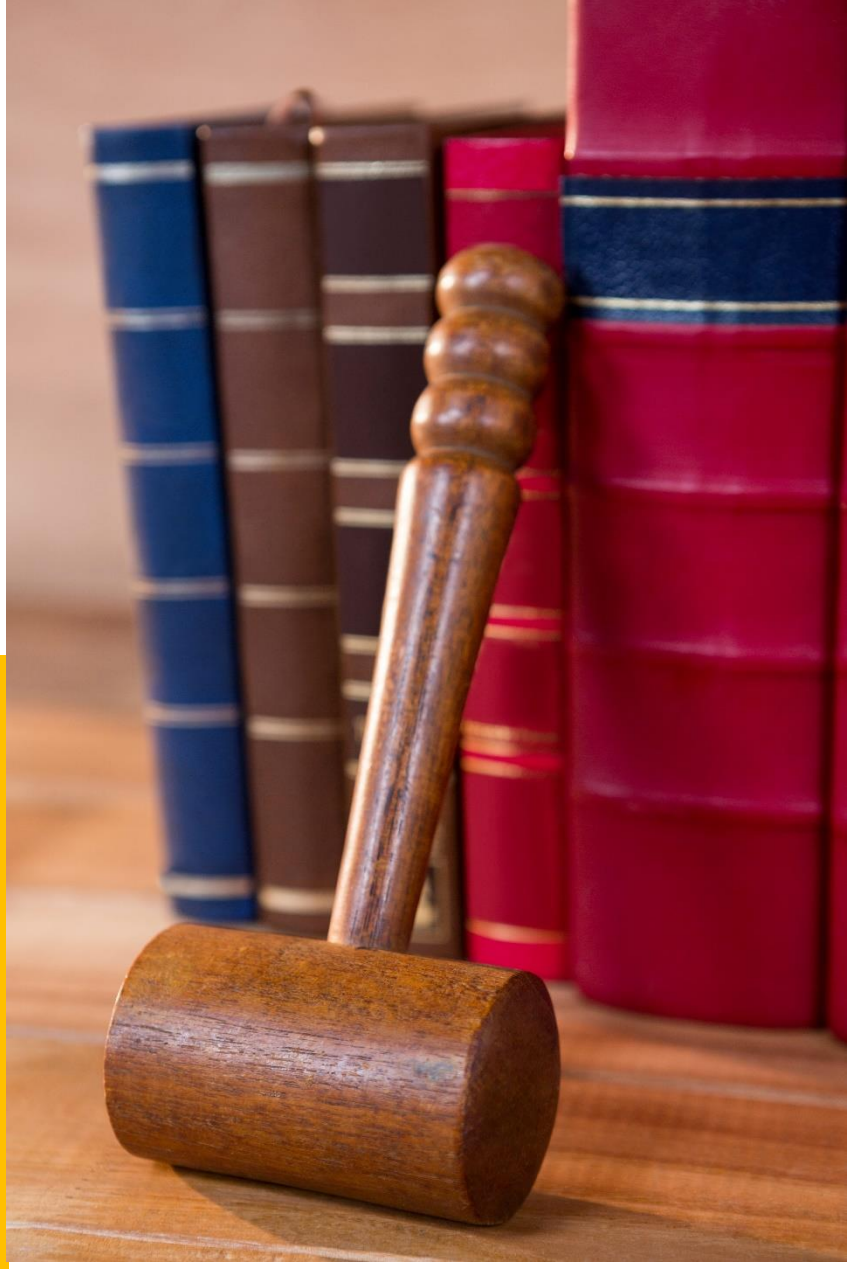
Lois et réglementations
Liste non exhaustive :

FRANCE

- **Loi Matras :** https://www.vie-publique.fr/loi/280089-loi-matras-25-novembre-2021-securite-civile-sapeurs-pompiers
- **Plan communal ou intercommunal de sauvegarde (Articles L731-3 à L731-5)** https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025506822/#LEGISCTA000044375302
- **LIVRE VII : SÉCURITÉ CIVILE (Articles L711-1 à L768-2)** https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025506654/#LEGISCTA000025507275
- **Ministère de l'Intérieur et des Outres-mers :** https://www.interieur.gouv.fr/Le-ministere/Securite-civile/Documentation-technique/Planification-et-exercices-de-Securite-civile

QUÉBEC

- **Loi sur la sécurité civile (Québec) :** https://www.legisquebec.gouv.qc.ca/fr/document/lc/s-2.3#:~:text=1.,la%20situation%20apr%C3%A8s%20l'%C3%A9v%C3%A9nement.
- **Loi sur la protection civile (Québec) :** https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-33
- **Loi sur la protection des personnes et des biens en cas de sinistre (Québec) :** https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-38.1/19991022
- **Loi sur les mesures d'urgence (Canada) :** https://laws-lois.justice.gc.ca/fra/lois/e-4.5/index.html
- **Loi sur la gestion des urgences (Canada) :** https://laws-lois.justice.gc.ca/fra/lois/e-4.56/
- **Loi sur les cités et villes (Québec) :** https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-19



Il est essentiel de comprendre ces lois et règlements afin de s'y conformer et de s'assurer que les actions entreprises sont en accord avec les exigences légales.

Comment se conformer à ces exigences tout en répondant efficacement aux crises

Se conformer aux exigences légales tout en répondant efficacement aux crises peut être un défi pour les villes. Il est essentiel de mettre en place des processus et des mécanismes de conformité appropriés.

Cela peut inclure la création et la mise à jour régulière de plans de gestion de crise, l'identification des responsabilités et des rôles clés, la formation du personnel sur les exigences légales, la réalisation d'exercices et de simulations pour tester la conformité, et la mise en place de mécanismes de suivi et d'évaluation.

Il est également important de maintenir une veille réglementaire pour être informé des évolutions législatives et réglementaires pertinentes.

Cela permet d'adapter les pratiques et les politiques de gestion de crises en fonction des nouvelles exigences.

Comment les maires peuvent anticiper et se préparer à ces défis futurs

Pour anticiper et se préparer aux défis futurs, les maires peuvent adopter plusieurs stratégies :

- **Surveillance et veille :** Il est important de rester informé des tendances émergentes, des études et des rapports pertinents dans des domaines tels que les changements climatiques, la sécurité informatique, la santé publique, etc. La surveillance constante permet d'identifier les menaces potentielles et de prendre des mesures préventives appropriées.

  Par exemple, en surveillant les données météorologiques et les modèles climatiques, les maires peuvent anticiper les risques accrus de tempêtes violentes ou de sécheresses prolongées.

- **Évaluation des vulnérabilités :** Les maires doivent évaluer les vulnérabilités propres à leur ville face aux tendances futures identifiées. Cela peut inclure une évaluation des infrastructures critiques, des ressources naturelles, des systèmes de communication, des services de santé, etc. Cette évaluation permet de comprendre les points faibles et de mettre en place des mesures de préparation ciblées.

  Par exemple, une ville, située dans une zone à risque d'inondation, peut investir dans des infrastructures de drainage améliorées pour réduire les impacts des précipitations accrues.

- **Planification proactive :** Les maires doivent intégrer les tendances futures dans leur planification de gestion de crises. Cela implique l'élaboration de scénarios de crise adaptés aux tendances identifiées, la mise à jour des plans d'urgence et des protocoles de réponse, ainsi que l'investissement dans les ressources et les capacités nécessaires pour faire face aux défis futurs.

  Par exemple, mettre en place des mesures de cybersécurité renforcées pour se prémunir contre les attaques informatiques.

- **Collaboration et partenariats :** Les maires doivent développer des collaborations et des partenariats avec d'autres acteurs, tels que les gouvernements régionaux, les agences gouvernementales, les organisations non gouvernementales et les entreprises privées. Ces partenariats peuvent renforcer la capacité de préparation et de réponse aux crises futures en tirant parti des ressources et des expertises complémentaires.

  Par exemple, une ville peut établir des partenariats avec des entreprises de technologie pour mettre en place des systèmes de surveillance avancés ou travailler avec des organisations humanitaires pour élaborer des plans d'intervention d'urgence.

“ Seul, nous pouvons faire si peu; ensemble, nous pouvons faire beaucoup. ”

Helen Keller

Réaliser un bon plan de communication

Centralisation de la communication

La centralisation de la communication en temps de crise permet de garantir la cohérence et la précision des informations diffusées. En désignant un point central ou un responsable de la communication, il est possible de s'assurer que les messages proviennent d'une source officielle et qu'ils sont alignés avec les objectifs et les stratégies de gestion de crise de la ville. Une communication centralisée facilite également la coordination des informations provenant de différentes sources et contribue à éviter la diffusion de fausses informations qui pourraient semer la confusion dans le public.

Importance de la communication transparente et régulière

La communication transparente et régulière est d'une importance capitale lors d'une crise. Les citoyens ont besoin d'informations claires et précises sur la situation, des mesures prises par la ville et des instructions à suivre. Une communication ouverte et honnête contribue à maintenir la confiance du public, à réduire l'anxiété et à prévenir la propagation de fausses informations. Il est essentiel de fournir des mises à jour régulières, de répondre aux questions et aux préoccupations du public, et d'expliquer les décisions prises.

Personnalisation des communications

Il est crucial de personnaliser les communications en fonction des destinataires afin de répondre à leurs besoins particuliers. Chaque segment de la population peut avoir des préoccupations différentes et nécessiter des informations adaptées à leur situation. Par exemple, il peut être nécessaire de fournir des messages dans différentes langues, d'adapter les informations pour les personnes ayant des besoins particuliers ou d'utiliser les canaux de communication préférés par certains groupes. En personnalisant les communications, on renforce l'engagement du public et on favorise une meilleure compréhension et adhésion aux mesures et instructions communiquées.

Outils et canaux de communication en cas de crise

La diversité des outils et des canaux de communication est essentielle pour atteindre un large public et s'adapter aux préférences individuelles. Cela peut inclure des alertes et des notifications d'urgence via des applications mobiles, des messageries instantanées (SMS), des réseaux sociaux, des sites Web, avec des communiqués de presse, des affiches, des conférences de presse, des réunions publiques, etc. Il est important d'utiliser des canaux multiples et complémentaires pour atteindre différents segments de la population, y compris les personnes ayant des besoins particuliers ou des barrières linguistiques.

Gestion des relations avec les médias

Les médias jouent un rôle clé dans la diffusion de l'information lors d'une crise. Il est essentiel d'établir et de maintenir de bonnes relations avec les médias locaux et nationaux. Cela comprend de nommer un porte-parole officiel de la ville, de fournir des informations régulières et précises aux médias, de tenir des conférences de presse, de répondre rapidement aux demandes d'interviews et de mettre à leur disposition des ressources médiatiques telles que des communiqués de presse et des dossiers d'information.

Évaluation et amélioration continue

L'évaluation et l'amélioration continue sont des éléments essentiels de la gestion de crises. Elles constituent le cœur d'une stratégie résiliente, permettant d'analyser en profondeur les succès et les échecs, d'affiner les plans existants et de développer des compétences et des outils adaptés à la nature évolutive des défis. C'est grâce à cette démarche itérative et réfléchie que les villes peuvent non seulement survivre aux crises, mais également en sortir plus fortes et mieux préparées pour l'avenir.

- **Importance de l'évaluation post-crise :** L'évaluation post-crise permet de tirer des enseignements précieux et de renforcer la résilience de la ville pour faire face à d'éventuelles crises futures. Il est essentiel de mener une évaluation approfondie pour comprendre les succès, les lacunes et les leçons apprises lors de la gestion de la crise. Cela permet de mettre en évidence les points forts à solidifier et les domaines à améliorer, afin de mieux se préparer et de mieux répondre aux crises à venir.
- **Méthodes pour analyser la performance du plan de continuité :** Plusieurs méthodes peuvent être utilisées pour analyser la performance du plan de continuité des activités (PCA, PCS, etc.) et évaluer son efficacité. Cela peut inclure l'examen des procédures et des protocoles utilisés pendant la crise, l'analyse des actions et des décisions prises, ainsi que la collecte de retours d'expérience de tous les acteurs impliqués. Des outils tels que les rapports d'incident, les évaluations après-action et les enquêtes auprès des parties prenantes peuvent être utilisés pour recueillir des données et évaluer la performance du plan de continuité.
- **Processus d'amélioration continue :** L'amélioration continue est essentielle pour s'adapter aux changements et pour renforcer la résilience face aux crises futures. Après avoir évalué la performance du plan de continuité, il est important de mettre en place un processus d'amélioration continue. Cela peut inclure la mise à jour des procédures et des protocoles en fonction des leçons apprises, la formation et le développement des compétences du personnel, l'identification des lacunes en matière de ressources et d'infrastructures, ainsi que l'amélioration des processus de communication et de coordination.

Il est gagnant de promouvoir une culture d'apprentissage et d'adaptation, où chaque crise est une occasion d'apprendre et de s'améliorer. En mettant en place un système d'évaluation régulier, en encourageant la rétroaction des parties prenantes et en prenant des mesures pour corriger les problèmes identifiés, les maires peuvent renforcer la préparation et la réponse aux crises, et maintenir une amélioration continue pour faire face aux défis futurs.

C'est grâce à cette démarche itérative et réfléchie que les villes peuvent non seulement survivre aux crises, mais également en sortir plus fortes et mieux préparées pour l'avenir.

Financement et ressources

La gestion de crises nécessite des ressources financières adéquates pour mettre en œuvre des plans de continuité efficaces. Voici quelques sources potentielles de financement pour soutenir la préparation et la réponse aux crises, ainsi que des stratégies pour maximiser l'utilisation des ressources disponibles.

- **Sources potentielles de financement :** Les maires peuvent explorer différentes sources de financement pour soutenir leurs efforts de gestion de crise. Cela peut inclure des fonds gouvernementaux, des subventions et des programmes dédiés à la préparation aux crises et à la continuité des services. Il est essentiel de rechercher les opportunités de financement disponibles au niveau local, régional, national et international. Les partenariats public-privé et les collaborations avec des organisations philanthropiques peuvent également offrir des opportunités de financement supplémentaires.
- **Maximiser l'utilisation des ressources disponibles :** Il est important d'optimiser l'utilisation des ressources disponibles pour répondre aux besoins liés à la préparation et à la gestion de crises. Cela peut impliquer une évaluation minutieuse des ressources existantes, y compris les infrastructures, les équipements, le personnel et les compétences. Les maires peuvent identifier les lacunes et les besoins prioritaires, puis développer des stratégies pour combler ces lacunes en maximisant les ressources existantes. Par exemple, ils peuvent optimiser l'utilisation des infrastructures municipales pour les opérations de secours, renforcer les compétences du personnel existant par le biais de formations ciblées, ou établir des partenariats avec des entreprises locales pour partager des ressources.
- **Collaboration intersectorielle :** La collaboration entre les différents secteurs et acteurs peut également contribuer à maximiser l'utilisation des ressources disponibles. Les maires peuvent travailler en étroite collaboration avec les entreprises privées, les organisations non gouvernementales, les établissements d'enseignement et d'autres entités pour partager les ressources et les compétences. Par exemple, les entreprises locales peuvent contribuer en fournissant des services ou des équipements essentiels, les organisations non gouvernementales peuvent apporter une expertise précise, et les établissements d'enseignement peuvent contribuer à la recherche et au développement de solutions innovantes.
- **Approche basée sur les priorités :** Une approche basée sur les priorités est essentielle pour maximiser l'utilisation des ressources disponibles. Les maires doivent évaluer les risques et les impacts potentiels des crises, puis allouer les ressources en fonction de ces priorités. Cela peut impliquer une planification stratégique à long terme pour identifier les domaines clés qui nécessitent des investissements et une attention particulière. En hiérarchisant les ressources en fonction des besoins les plus critiques, les maires peuvent optimiser l'utilisation des ressources disponibles pour renforcer la préparation et la réponse aux crises.

Conclusion

Pour conclure, ce dossier a traité des aspects majeurs de la gestion de crises par les responsables municipaux. Nous avons navigué à travers les diverses phases de préparation et de planification, soulignant l'importance de l'appréciation des risques, de l'élaboration de plans de continuité et de l'engagement significatif de la communauté.

L'accentuation de la fréquence, de la complexité et de l'imprévisibilité des crises nécessite une préparation en amont. En tant que maires, l'anticipation des enjeux futurs, la détection des tendances naissantes et l'ajustement de vos stratégies sont des impératifs. L'implication de la communauté, l'intercommunalité, la gestion des collaborations externes et le travail de concert avec les intervenants locaux sont des facteurs clés pour accroître la résilience et la capacité de réaction face aux crises.

Nous avons par ailleurs mis en exergue la nécessité de la gestion des ressources humaines, d'une communication transparente, du respect des lois et des règlements, ainsi que l'évaluation et l'amélioration constante. Ces facteurs participent à renforcer la préparation, à maximiser l'utilisation des ressources disponibles et à augmenter l'efficacité du plan de continuité.

Vous, en tant que maires, jouez un rôle central dans la gestion des crises au sein de vos villes. En tant que leaders, vous êtes chargés de prendre des décisions avisées, de mobiliser les ressources requises et de coordonner les efforts de préparation et de réaction. Vous êtes les garants de la sécurité et du bien-être de votre communauté.

Il est donc crucial que vous mettiez en action les connaissances acquises à travers ce document. Mobilisez vos équipes, engagez activement votre communauté, renforcez les partenariats avec les acteurs locaux, planifiez de manière proactive, et améliorez la résilience et la préparation de votre ville. Ensemble, nous pouvons faire face aux crises futures et bâtir un avenir plus sûr et résilient pour nos communautés.

Nous vous encourageons à vous servir de ce dossier comme une référence pour votre travail de maire. La gestion de crises est une tâche ardue, mais une préparation robuste, une collaboration étroite et une vision proactive permettront de surmonter ces défis et d'assurer la sécurité et la continuité des services essentiels pour nos villes.

Soyez le leader inspirant qui oriente votre ville vers la résilience et la préparation aux crises futures. Ensemble, nous pouvons construire un avenir plus sûr, plus solide et plus résilient pour tous.

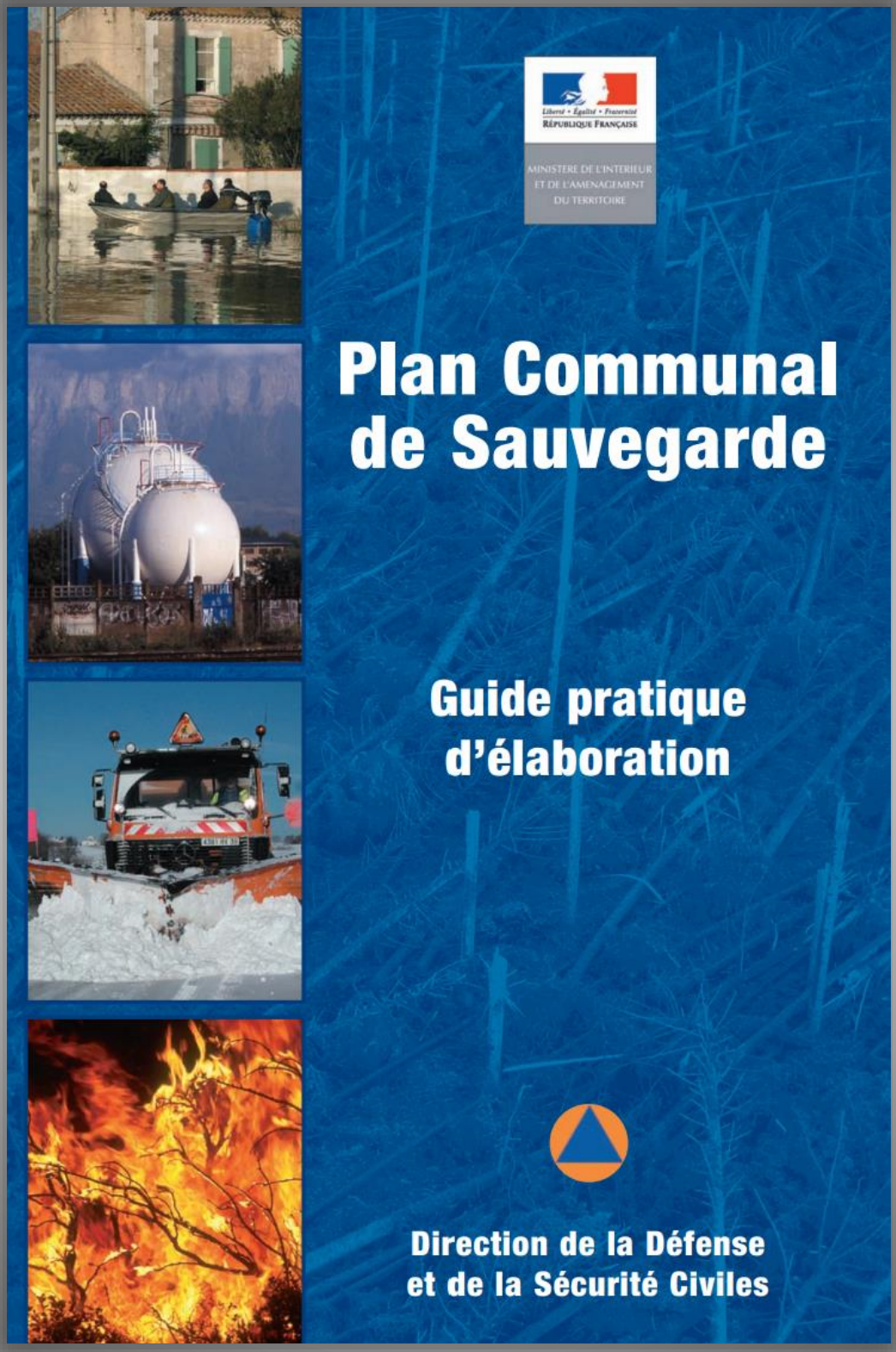
Alexandre Fournier et Karine Maréchal

Avez-vous lu les autres dossiers du mois ?

Janvier 2023

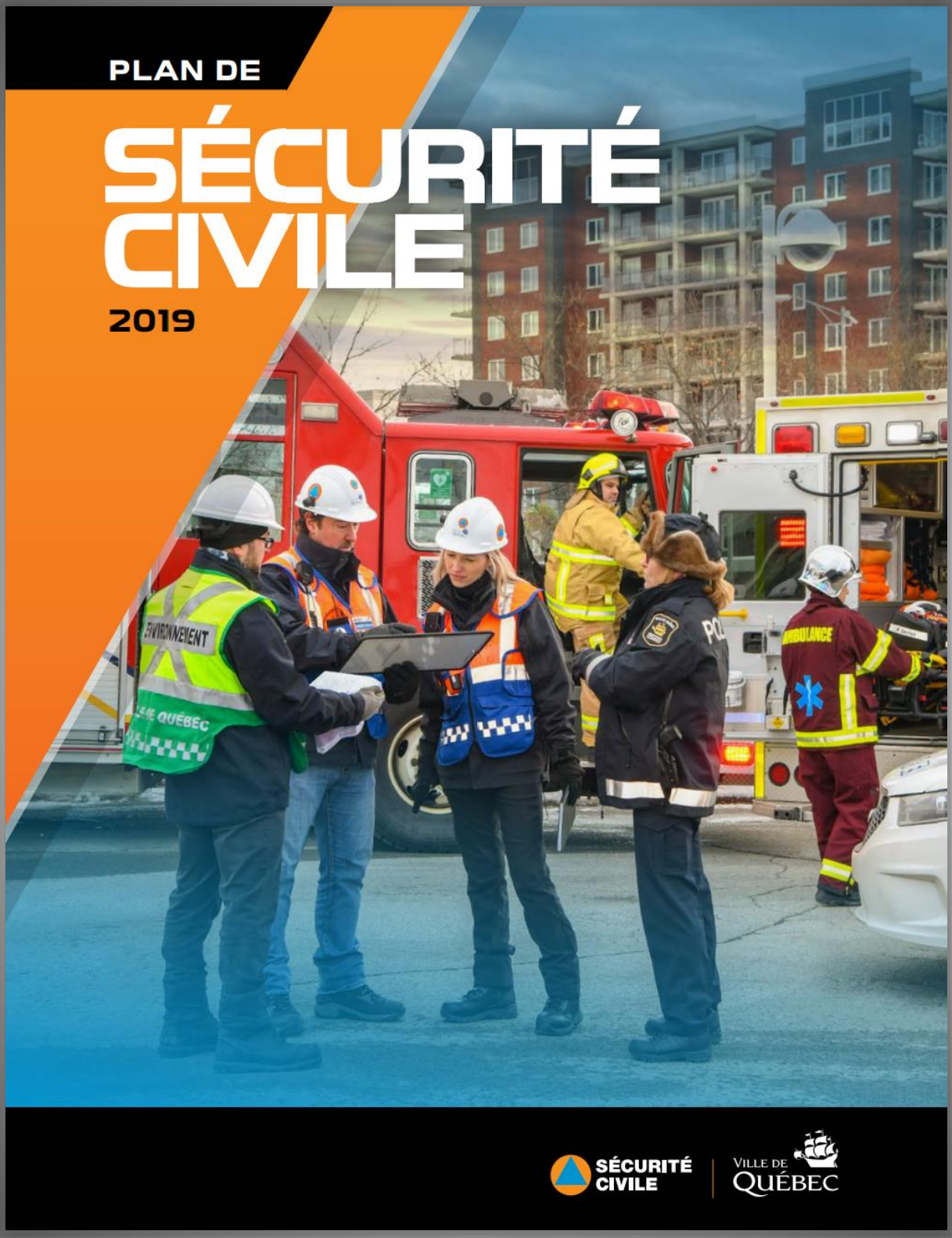
Avril 2023

Profitez de vos vacances pour lire



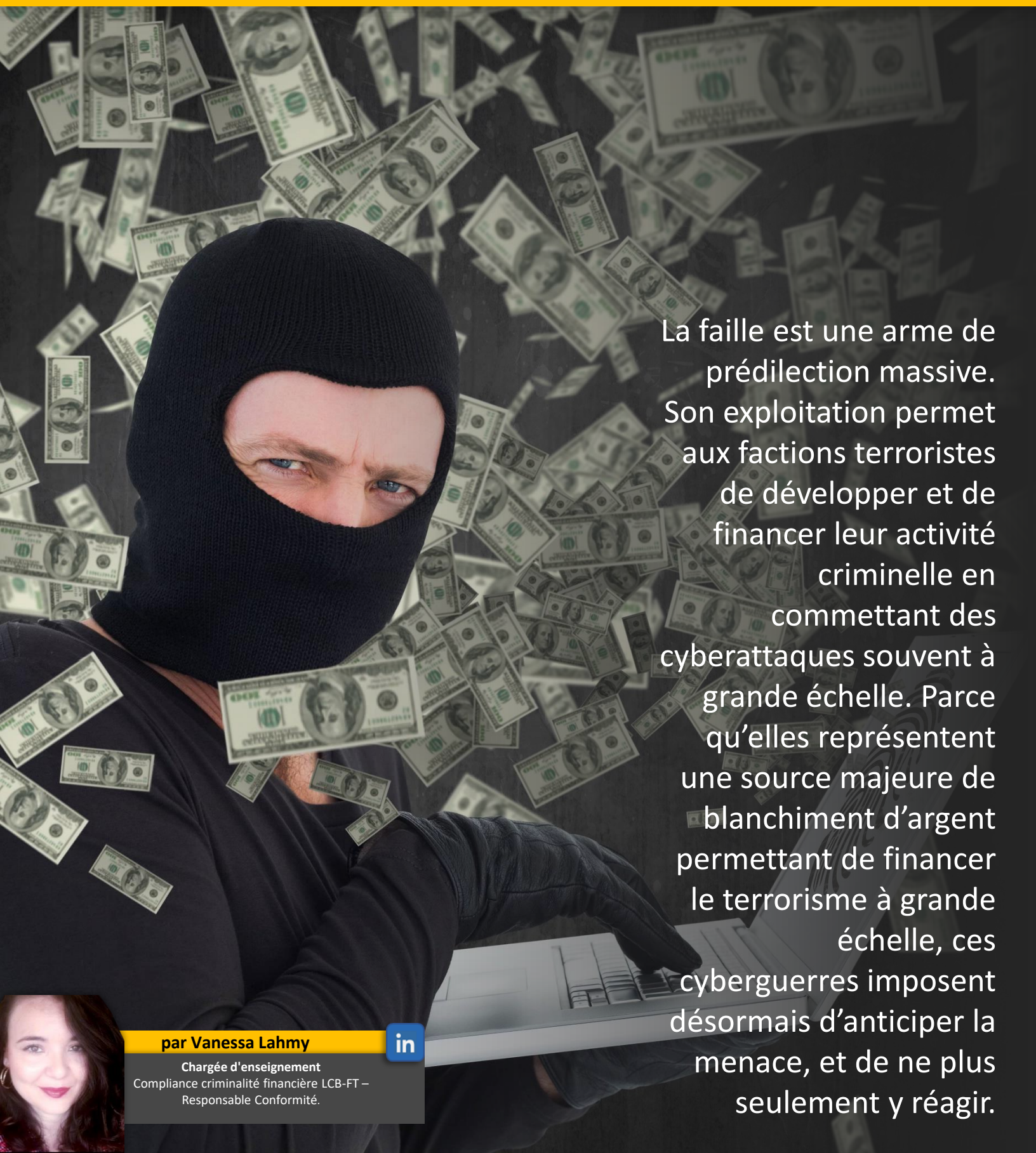
Lire ce plan

Profitez de vos vacances pour lire



Lire ce plan

Cyberterrorisme et blanchiment d'argent : agir plutôt que réagir



La faille est une arme de prédilection massive. Son exploitation permet aux factions terroristes de développer et de financer leur activité criminelle en commettant des cyberattaques souvent à grande échelle. Parce qu'elles représentent une source majeure de blanchiment d'argent permettant de financer le terrorisme à grande échelle, ces cyberguerres imposent désormais d'anticiper la menace, et de ne plus seulement y réagir.

par Vanessa Lahmy

Chargée d'enseignement
Compliance criminalité financière LCB-FT – Responsable Conformité.

La faille est une arme de prédilection massive.

Son exploitation permet aux factions terroristes de développer et de financer leur activité criminelle en commettant des cyberattaques souvent à grande échelle.

Parce qu'elles représentent une source majeure de blanchiment d'argent permettant de financer le terrorisme à grande échelle, ces cyberguerres imposent désormais d'anticiper la menace, et de ne plus seulement y réagir.

Les cyberattaques, sources de blanchiment d'argent et de financement du terrorisme

L'attaque par rançongiciel -ransomware- permet de comprendre clairement le lien unissant cyberterrorisme et blanchiment d'argent.

Après avoir effectué une enquête sur la cible visée, le hacker va louer ou pirater un hébergeur de serveurs, avant d'opérer depuis ces serveurs anonymisés afin de laisser le minimum de traces(1) .

L'attaque peut alors se dérouler en passant par l'envoi de mails frauduleux, des sites malveillants ou encore des clés USB corrompues infiltrées via un complice.

Les données sont ensuite cryptées, et la demande de rançon en cryptomonnaies - afin de contourner les régulations mises en place par le secteur bancaire - est envoyée à la cible(2) .

Pour faire pression sur la victime, le hacker peut menacer de rendre publiques les données les plus sensibles.

Une fois la rançon récupérée, il fera appel à un vaste réseau lui permettant de blanchir parfois jusqu'à plusieurs millions d'euros en cryptomonnaies:

- **les "mixers"** vont d'abord mélanger l'argent sale issu de la rançon avec de la cryptomonnaie légale afin de la rendre intraçable, avant que
- **les "mules"** ne fassent circuler les gains et les convertissent en argent propre(3) - achat d'armes et de logistique servant un dessin terroriste puis revente, conversion dans des pays où la législation LCB-FT est plus souple-.

Tous les revenus sont partagés sur des comptes en cryptomonnaies visibles et faciles à contrôler.

Face à cette menace d'envergure, il devient urgent d'agir… mais différemment.

Cyberterrorisme et blanchiment d'argent imposent une action anticipée

Si la monnaie virtuelle est l'avenir, ses lendemains ne seront prometteurs que si elle est correctement, pleinement régulée...et à temps.

En effet, les cryptomonnaies facilitent l'alimentation des réseaux terroristes et le financement de leur dessein criminel, en restant invisibles des autorités répressives, puisque " (…) le fait d'être payés en cryptomonnaies leur garantit un quasi-anonymat« (3).

Ainsi, au lieu de passer par l'intermédiaire d'un portefeuille géré par une plateforme externe, le groupe terroriste palestinien "les Brigades Izz al-Din al-Qassam" a créé des portefeuilles via une plateforme sous leur contrôle, s'inspirant ainsi du financement occulte mis en place par l'État islamique.

Certes, convertir des sommes faramineuses de litecoins en argent réel et les rapatrier sur des comptes bancaires attirerait non seulement l'attention des services de police anti-blanchiment, mais aussi du banquier, qui, en tant que Professionnel du Secteur Financier (PSF) et "entité obligée" selon les directives européennes anti-blanchiment est soumis à un devoir constant de vigilance à l'égard de ses clients (procédures KYC et Client Due Diligence).

Néanmoins, le recours au dark Net permet aussi de blanchir les cryptomonnaies : moyennant une commission, ils peuvent ainsi " (…) utiliser une carte bancaire créditée de plusieurs dizaines de milliers de dollars en payant son propriétaire en bitcoins, éthers ou litecoins"(4).

S'ils ne peuvent pas entrer par la porte, les cybercriminels trouveront toujours un moyen de passer par une fenêtre, tant que le champ de vision des décideurs de ce monde ne sera pas élargi.

Même si les mesures énergiques prises récemment par l'Union européenne visant à contrer l'utilisation abusive de cryptoactifs sont salutaires(4), elles surviennent pour autant trop tardivement et ne s'avèrent pas suffisantes.

Les instances européennes ne peuvent plus se contenter de répondre aux menaces au fur et à mesure par de nouvelles réglementations relatives à la cybersécurité et à la cyberrésilience : elles doivent aller au-delà, en encadrant plus rapidement l'usage détourné de l'intelligence artificielle et en anticipant de manière plus générale les prochains impacts de cette crise à horizon lointain, et non plus à court terme.

Car le facteur temps est un paramètre fondamental à prendre en considération pour tenter de freiner ces infractions.

A chaque État membre ensuite d'instaurer un cadre réglementaire national pertinent, et aux opérateurs économiques de le mettre en œuvre de façon efficace, à condition pour cela d'être doté d'une gouvernance interne qui soit suffisamment robuste.

À l'ère d'un nouvel ordre mondial complexe et crisogène, il est donc indispensable d'avoir une longueur d'avance sur les cybercriminels organisés sur le modèle d'une entreprise qui ne connaît pas la crise !

Plutôt que de réagir a posteriori à la menace, l'heure est venue pour chaque opérateur économique, en fonction de son contexte professionnel, d'agir a priori en anticipant les problématiques qu'il serait susceptible de rencontrer et en imaginant, pour chaque scénario envisagé, un large spectre des réponses opérationnelles à mettre en œuvre.

Article écrit par Vanessa Lahmy

Trois clés pratiques qui ont fait leurs preuves

Maintenez régulièrement à jour votre cartographie des risques et échangez différents points de vue entre collègues.

Formez-vous...et informez-vous régulièrement.

Surtout, envisagez votre fonction professionnelle de manière transversale et restez connectés à votre département informatique !

Référence du texte :

(1)MONNET Bertrand. La faille, arme du cybercriminel. Les mafias : quand le crime organisé menace le monde, mai-juillet 2022, Hors-série, p.46.

(2)HOUEIX Romain. Les cryptomonnaies, nouvelle arme des groupes terroristes ? (en ligne) , disponible sur https://www.france24.com/fr/20190822-bitcoin-cryptomonnaie-jihadistes-terrorisme-brigade

(3)KRIM, Mourad. Suivez l'argent : comment les cybercriminels blanchissent le fruit de leurs vols à grande échelle (en ligne). Disponible sur https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/suivez-largent-commentles-cybercriminels-blanchissent-le-fruit-de-leurs-vols-a-grande-echelle/

(4)Conseil de l'UE, Communiqué de presse du 29 juin 2022, disponible sur https://www.consilium.europa.eu/fr/press/press-releases/2022/06/29/anti-money-launderingprovisional-agreement-reached-on-transparency-of-crypto-asset-transfers/;
Conseil de l'UE, Communiqué de presse du 16 mai 2023, disponible sur https://www.consilium.europa.eu/fr/press/press-releases/2023/05/16/anti-money-launderingcouncil-adopts-rules-which-will-make-crypto-asset-transfers-traceable/ Conseil de l'UE, Communiqué de presse du 7 décembre 2022, disponible sur https://www.consilium.europa.eu/fr/press/press-releases/2022/12/07/anti-money-launderingcouncil-agrees-its-position-on-a-strengthened-rulebook/

Vanessa Lahmy Fondatrice de VL CONSULTING
Analyse juridique gouvernance/ business / droits de l'homme, criminalité financière /lutte anti-blanchiment / contre financement du terrorisme, compliance, géopolitique, Relations européennes et internationales - Europe, Israël, E.A.U, Asie

VL CONSULTING , Services prestés en France et à l'international : Formations professionnelles et enseignement en Droit – Conformité /LCB-FT Accompagnement des entreprises du secteur financier dans l'élaboration, le déploiement et la mise à jour de leur programme conformité.
Tel: +352 621 711 272
Email: esther.lahmy@gmail.com

Préparez votre entreprise aux crises avec l'intelligence artificielle

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

Élaborer un plan de gestion de crise optimisé pour vous

Évaluer vos risques en fonction d'un contexte particulier

Établir des scénarios de crise en fonction de vos risques

Entraîner vos équipes sur la base de vos scénarios de crises

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

Pierre-Henri D.

Inscrivez-vous dès maintenant

INSCRIPTION

https://bit.ly/3zrv3vR

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

Apprendre de la tourmente…
parallèles avec une crise humanitaire

Le propre des crises est de nous tomber dessus sans prévenir.

Le vendredi 15 janvier 2010 en fin de journée, soit quatre jours après le tremblement de terre qui a détruit Port-au-Prince, je suis appelé dans une rencontre de logistique, car mon employeur, Vidéotron, est sur le point de dépêcher une équipe de deux personnes pour établir un centre de communication au cœur de la capitale dévastée. Après avoir discuté du matériel minimal pour l'opération, on me demande d'être de l'équipe et on m'informe que le départ est prévu pour le lendemain matin. Sans vraiment trop y penser, c'est oui : pas question de passer à côté de cette expérience. Malgré l'improvisation entourant notre intervention sur le terrain à la suite du tremblement de terre de 2010 en Haïti, notre manière de naviguer dans la crise m'a souvent servi de points de référence dans les discussions apparentées au sujet dans le secteur des TI.

La soirée et la nuit sont occupées par une préparation frénétique en vue du départ. Mon matériel personnel ressemble à celui que j'ai normalement avec moi lorsque je fais de la longue randonnée, incluant une boussole que je traîne par habitude et qui s'avérera très utile.

par Bruno Germain

Architectures, implementations, public speaker

Le matin, sur le tarmac, nous chargeons le matériel dans l'avion privé de monsieur Péladeau et nous devons nous rendre à l'évidence : nous allons devoir laisser du matériel derrière. Après un tri de dernière minute pour choisir deux unités fixes et une unité mobile de communication satellite, repaquetage, approbation des pilotes pour le poids du cargo et nous décollons. Nous allions découvrir, une fois arrivés, que dans notre hâte, nous n'avions pas porté la même attention aux besoins des « deux humains » qu'aux systèmes de communication. Il nous faudra improviser, ne serait-ce que pour manger les sachets de nourriture déshydratée.

En passant par la République dominicaine où deux camionnettes nous attendent, nous arrivons à Port-au-Prince le dimanche en fin d'après-midi. La ville est dévastée, des corps gisent dans les rues et les gens errent ou fouillent les décombres. Nous prenons la mesure de ce qui nous attend : c'est très différent d'en entendre parler à la télévision que d'être plongé dedans.

Nous passons plusieurs jours à parcourir la ville pour trouver une maison qui a résisté au séisme et avoir une entente avec le propriétaire afin d'y installer les antennes et le centre de communication.

La maison trouvée, nous nous mettons au travail. Nous adaptons continuellement nos façons de faire, car installer le tout selon « les meilleures pratiques » est impossible. Arrive le moment de pointer la première soucoupe vers le ciel et de trouver le satellite : l'appareil permettant d'ajuster l'orientation, l'élévation et l'angle de rotation du récepteur est resté à Montréal. Un peu découragés, nous brainstormons et je finis par proposer d'utiliser ma boussole et un cadran découpé dans un morceau de carton pour faire nos ajustements. C'était tellement low tech et saugrenue comme idée, mais nous n'avions aucune option de rechange.

Nous allumons la génératrice pour alimenter le système. En ligne sur le téléphone satellite mobile avec le groupe des opérations à Montréal, nous commençons à faire nos ajustements en espérant établir le lien : il nous faut trouver un signal de 10-16w dans un ciel ouvert. Une trentaine de minutes plus tard, le lien est établi et nous pourrons, dans les jours qui suivront, inviter la société civile et les médias de Port-au-Prince à utiliser le centre de communication pour coordonner les efforts sur le terrain et pour communiquer avec la diaspora haïtienne et le monde en général.

Le bouche-à-oreille étant particulièrement efficace et en vogue à l'époque à Port-au-Prince, nous avons aussi reçu une invitation des gens de Télécoms Sans Frontières installés sur la base onusienne à l'aéroport, pour les aider à monter leurs propres installations devant servir aux ONG.

Notre dernière tâche fut d'instruire une équipe locale sur le fonctionnement du centre et de passer la main. Il ne nous restait plus qu'à retourner à Montréal, heureux de notre modeste contribution et riches de cette expérience unique dans nos vies.

"Now climb young Grasshopper, so your Kung Fu won't be weak." *

Maintenant, grimpez jeune sauterelle, pour que votre Kung Fu ne soit pas faible.

Se préparer à une crise dans le monde des TI est absolument nécessaire, car la probabilité d'un incident avoisine 100 %. Comme dans notre voyage, le niveau de préparation variera d'une organisation à l'autre, mais j'ose espérer qu'au sein de vos équipes, vous avez déjà identifié les joueurs clés qui seront en mesure de naviguer avec le stress, les incertitudes, la politique, les embûches avec facilité et faire preuve de flexibilité et de créativité pour vous sortir de la crise.

Article écrit par Bruno Germain

Quelques pépites de sagesse transférables aux TI :

Mon directeur de l'époque savait exactement qui il voulait envoyer à Haïti lorsqu'il est venu me chercher. Il en va de même pour une cellule de crise : n'en laisser pas la composition au hasard.

Ça n'ira pas comme prévu, ce qui ne veut pas dire de ne pas planifier. En revanche, ce que cela veut dire, c'est que nous aurons besoin de gens d'expérience ET avec l'ouverture d'esprit nécessaire pour nous adapter et envisager des solutions possiblement inédites.

Évaluer les idées proposées au mérite.

Ne pas attendre d'avoir l'approche parfaite avant d'agir pourvu que ça aille dans la bonne direction. Plutôt avoir une approche itérative pour s'améliorer avec le temps.

Quand une crise frappe, nous sommes tous dans la même équipe. Ne pas hésiter à partager nos expériences, nos approches et offrir notre aide à une autre organisation. Ou au contraire, à demander du soutien si nous sommes au bout de nos ressources.

Prévoir ce qu'il faut pour que les « humains » fonctionnent bien.

*Quel est le lien avec la citation de Maître Po de l'émission Kung Fu? Aucune, mais tous les livres sérieux ont ce genre de citations songées.

Bruno Germain Architecte de solutions chez Zscaler, 37 ans d'expérience dans la conception, la mise en œuvre, l'exploitation et la sécurisation d'infrastructures de télécommunication pour les centres de données, les intranets, les zones démilitarisées et les WAN mondiaux. Membre de l'équipe d'origine qui développe les normes IEEE 802.1ah et 802.1aq pour les réseaux virtualisés et fournit de nouvelles architectures de centre de données pour l'évolutivité et l'automatisation. Partage des brevets sur l'intégration de routeurs virtuels à ces normes et sur la virtualisation des centres de données. Architecte technique dans une organisation de développement commercial, responsable de l'engagement avec les DSI et les équipes techniques, d'identifier de nouvelles opportunités de marché et de fournir des spécifications pour d'autres améliorations de produits. PME fournissant un support de superposition aux équipes de vente du monde entier. Il est aussi … Amateur de plein air (et de bons moments, car la vie est courte), et passionné par les forces et les failles des architectures sécurisées.

Gestion de crise et intelligence artificielle : entre efficacité et limites

La révolution de l'intelligence artificielle qui s'annonce semble présenter à première vue de nombreux atouts dans la gestion de crise.

par Eric Przyswa

PhD, consultant (risk05)

Publishing contents, Writer | Public affairs | CSR-Ethics-Risks | Research, Industry, AI, Digital

Atouts de l'IA

On peut en effet distinguer trois avantages évidents liés à l'IA :

- Le premier est de pouvoir gérer d'importantes bases de données en un temps record. Cet atout prend toute sa dimension dans les crises qui concernent des régions qui ne bénéficient pas de données en tant que telles. L'utilisation de techniques cartographiques de pointe telles que MissingMaps(1) permet ainsi de collecter des données et de les visualiser sur des zones à risques dans les pays en voie de développement en déficit d'informations. L'IA a été associée à ces cartographies satellites pour aider certains pays africains tels que l'Ouganda à visualiser des infrastructures présentant des dangers tels que des ponts ou des routes.
- L'IA permet aussi d'anticiper des crises notamment liées à des pandémies. On peut citer ici l'exemple de la start-up canadienne Blue Dot Global(2) qui s'est spécialisée dans une technologie d'alerte précoce pour les maladies infectieuses. La société qui suit en permanence 150 maladies infectieuses dans le monde a été l'une des premières sources internationales à identifier les risques associés à la COVID-19.
- Dans le cas de catastrophes à venir particulièrement complexes, l'IA peut s'avérer être un outil précieux. Le cas des changements climatiques et l'atteinte d'objectifs ambitieux en matière de gaz à effet de serre est un exemple significatif. En effet, dans un tel contexte, l'IA peut aider à concevoir des politiques de transport ou de logement plus adaptées en optimisant l'utilisation de données liées à la mobilité ou à la consommation d'énergie des bâtiments.

Cela dit, si l'on refuse de céder aux sirènes de certains gourous de l'IA et autres leaders dits « transhumanistes », force est de reconnaître que l'IA présente encore aujourd'hui certaines limites, en particulier dans la gestion de crise.

Importance des crises hors normes et limites de l'IA

Il convient tout d'abord de rappeler une caractéristique des nombreuses crises contemporaines : la surprise stratégique. On retrouve ce concept de « surprise stratégique » dans la catastrophe de Fukushima (vagues du tsunami plus hautes que prévues, inondation de la centrale) ou dans le cas de la centrale nucléaire ukrainienne de Zaporijjia dont aucun scénario n'avait anticipé un conflit armé autour de la centrale. On peut tout à fait concevoir que même avec une IA puissante, de tels scénarios n'aient pu être anticipés.

Ce déficit d'anticipation peut aussi se mettre en corrélation avec le principe suivant lequel l'hyper complexification des systèmes industriels ne permet pas d'anticiper tous les scénarios possibles. Selon le sociologue Charles Perrow, la complexité interactive et le couplage serré (tight coupling) au sein du système industriel produiront inévitablement des accidents qualifiés de systémiques(3).

Sur le plan organisationnel, il est donc important de pouvoir intégrer une stratégie pivot face à des situations extrêmes hors normes(4) ou face à des crises systémiques, mais difficilement anticipables. Une telle stratégie pivot ne peut s'envisager stricto sensu dans le cadre d'une logique algorithmique. En situation extrême plusieurs facteurs mettraient en relief les limites de l'IA pour une telle gestion de crise. Les professeurs Bibard et Sabouret(5) insistent sur l'importance des émotions et des corps dans le rapport à l'IA. Or, on ne peut que constater que dans la gestion de nombreuses crises hors normes, l'importance de l'improvisation ainsi que d'une bonne gestion des émotions sont des points stratégiques non pris en compte de manière optimale par l'IA.

La comparaison avec les improvisations du jazz a notamment été décryptée sur le plan organisationnel par le théoricien Karl Weick(6) et peut tout à fait se décliner dans certaines gestions de crises extrêmes. Certes, l'IA pourrait s'affirmer comme un outil d'aide à la décision précieux, mais elle ne pourra pas remplacer l'importance de la perception des espaces, des émotions et d'un sens du tempo souvent essentiels en particulier dans une situation d'urgence non prévue.

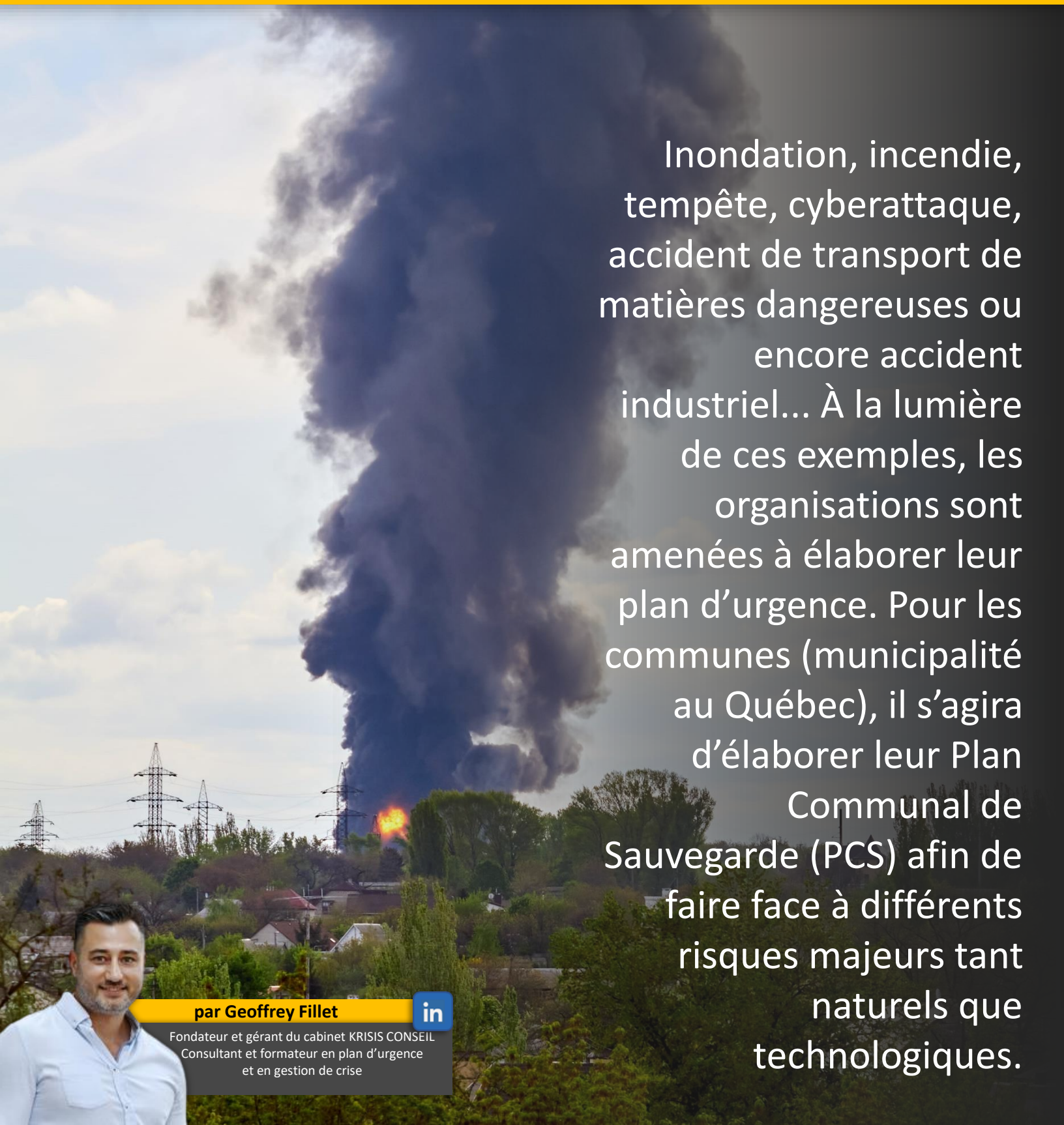
Dans un curieux paradoxe, le binôme « gestion de crise — IA » démontre donc à la fois les atouts de l'IA comme outil novateur, mais aussi ses limites, en particulier dans des démarches d'improvisation qui réaffirment la place centrale des émotions dans la gestion de certaines crises et où l'IA est, et restera pour un temps certain, en deçà de nos attentes.

Article écrit par Eric Przyswa

(1) https://www.missingmaps.org/fr/ MissingMaps a été lancé en 2014 par la Croix-Rouge américaine, la Croix-Rouge britannique, Médecins sans frontières et l'équipe humanitaire d'OpenStreetMap.
(2) https://bluedot.global
(3) C. Perrow, Normal Accidents, Living with High-Risk Technologies, Princeton University Press, 1999.
(4) Andrew Winston, « Resilience in a Hotter World », Harvard Business Review, avril 2014.
(5) L'intelligence artificielle n'est pas une question technologique, Laurent Bibard, Nicolas Sabouret, éditions de l'Aube, 2023.
(6) Karl E. Weick, « Improvisation as a Mindset for Organizational Analysis », Organization Science, 9(5), 1998.

Eric Przyswa est consultant en affaires publiques et management dans le secteur de l'IA, du numérique et des risques (risk05). Il est aussi impliqué dans des travaux éditoriaux qualitatifs et est écrivain. Il a été par le passé chercheur à Mines ParisTech et consultant marketing. Formation : Docteur en gestion, université Dauphine et Sciences Po Paris. https://www.risk-05.com
Il a aussi une expérience professionnelle dans plus de 15 pays. Il a travaillé à Singapour/Asean et en Allemagne/Europe centrale à des postes marketing et dans le conseil. Il a aussi été consultant et chercheur associé à MINES ParisTech en management et sécurité produit au sein de différentes industries (énergie, luxe, santé). Page de chercheur : https://www.researchgate.net/profile/Eric-Przyswa Il est auteur du livre "Contrefaçon-Cybercriminalité" aux éditions FYP (livre du jour Les Echos) et co-auteur d'un livre sur la gestion de crises aux éditions Mines ParisTech.

Réaliser son plan d’urgence pour qu’il soit réellement « opérationnel » le jour J!



Inondation, incendie, tempête, cyberattaque, accident de transport de matières dangereuses ou encore accident industriel... À la lumière de ces exemples, les organisations sont amenées à élaborer leur plan d’urgence. Pour les communes (municipalité au Québec), il s’agira d’élaborer leur Plan Communal de Sauvegarde (PCS) afin de faire face à différents risques majeurs tant naturels que technologiques.

par Geoffrey Fillet

Fondateur et gérant du cabinet KRISIS CONSEIL
Consultant et formateur en plan d’urgence
et en gestion de crise

Que vous soyez maire d'une commune ou dirigeant d'une entreprise, il vous est donc nécessaire d'élaborer une réponse opérationnelle pour faire face à ces événements au sein de votre organisation.

Par exemple, la mise en place d'un PCS, maillon local de l'organisation de la sécurité civile, permet aux communes de se préparer en se formant, en se dotant de modes d'organisation et d'outils techniques pour pouvoir faire face à toutes les situations de crise.

Même si le plan d'urgence n'est pas rendu obligatoire pour toutes les organisations, son élaboration est fortement conseillée.

S'il n'est pas réalisé seulement dans la volonté de cocher la case réglementation, sa mise en place s'avère précieuse pour faire face à tous types de situations d'urgence.

De plus, même si vous réalisez le plus beau plan d'urgence, si ce dernier est élaboré dans un coin puis relégué au fond d'un tiroir, il ne démontrera jamais son aspect opérationnel le jour J!

Alors pour vous aider à élaborer votre plan d'urgence de façon réellement opérationnelle, il vous est indiqué ci-dessous cinq conseils :

Élaborez un schéma d'alerte interne robuste

C'est la condition sine qua non pour une bonne gestion de la situation d'urgence. Vous avez certainement bien réfléchi à la meilleure organisation d'urgence, mais si personne n'est alerté en interne ou si on ne parvient pas à contacter les bonnes personnes, cette belle organisation ne servira à rien.

Dans un 1er temps, il faut se poser la question : comment votre organisation peut-elle être alertée d'une situation d'urgence?

Quelles sont les personnes ou entités qui doivent être contactées, par quels moyens, et ce à tout moment de la journée et de l'année?

Dans un 2e temps, il faut savoir comment mobiliser votre personnel en interne afin de vous structurer pour faire face à la situation. Un moyen pratique et visuel pour réaliser cette tâche est la réalisation d'un logigramme.

Pensez à prévoir plusieurs logigrammes en fonction des situations possibles : heures ouvrées ou non ouvrées, avec astreintes, etc. Le principe de l'alerte interne par l'appel en cascade (chaîne téléphonique) des acteurs concernés est une méthode à privilégier.

Sortez de votre bureau, allez au contact des futurs acteurs du plan

Trop souvent, les plans d'urgence sont élaborés en vase clos. Cela s'avère contre-productif, car il y a de fortes chances que face à la réalité du terrain votre plan soit au final inopérationnel.

Afin d'éviter cet écueil, il est primordial de prendre contact avec les différents acteurs qui seront concernés en cas de déclenchement du plan pour leur exposer votre objectif, vos idées et vos questionnements.

D'une part, vous les impliquerez dans la démarche d'élaboration, ils commenceront déjà à appréhender leur rôle et leur mission et d'autre part, ils vous aideront à trouver les solutions les plus adaptées à la réalité du terrain.

Même si le plan d'urgence n'est pas rendu obligatoire pour toutes les organisations, son élaboration est fortement conseillée.

Ne négligez pas les outils pratiques

Alors oui, le document du plan d'urgence en lui-même est très important et il faut bien respecter les différentes étapes structurantes de ce document, surtout quand elles s'avèrent réglementaires. Mais les outils pratiques ne sont vraiment pas à négliger.

Ce sont eux qui vont vous épauler, vous aider à prendre des décisions durant la situation d'urgence, sur le terrain, dans le feu de l'action. Ils vont aussi vous permettre de retranscrire la situation de façon visuelle et donc, de favoriser une meilleure compréhension pour tous les acteurs. On retrouve différents outils pratiques :

- Outils d'aide à la décision (fiches réflexes, fiche d'alerte ou communiqué de presse à trous, etc.)
- Tableaux de bord à afficher en cellule de crise, chasubles (gillet de sécurité), etc.
- Outils de communication (téléphone fixe ou mobile, radios)
- Annuaires de crise
- Cartographies et plans opérationnels

Sensibilisez, formez et exercez vos collaborateurs

Par la sensibilisation, il est question de faire prendre conscience de l'objectif final que représente le plan d'urgence. Il est important que tout le monde puisse se projeter grâce à un discours clair et simple.

Ensuite, il faut former les acteurs. Dans votre plan, vous allez désigner des personnes qui devront tenir des rôles et des missions au sein de l'organisation d'urgence. Il va donc falloir former ces personnes afin qu'elles maîtrisent ce que l'on attend d'elles en cas de déclenchement du plan.

Enfin, il est primordial d'exercer tous les acteurs. La réalisation d'un exercice se trouve être la meilleure méthode pour éprouver l'opérationnalité de votre plan d'urgence. Il permet d'entraîner les acteurs aux comportements et tester les connaissances attendues, et comporte l'avantage de contribuer à la mise à jour régulière de votre plan. Et puis, sans exercice, comment savoir si ce que vous avez produit sur le papier s'avère opérationnel sur le terrain?

Connaissez les attentes des pompiers et sachez communiquer avec eux

C'est quelque chose à laquelle on ne pense pas forcément quand on élabore le plan d'urgence. On se consacre à rendre la meilleure copie possible, mais on ne se projette pas concrètement dans la situation d'urgence qui nécessite une réelle collaboration avec les pompiers.

Vous avez tout intérêt à venir vous positionner en « facilitateur » auprès des secours afin que leur intervention se déroule dans les meilleures conditions. N'oubliez pas qu'ils ne connaissent que très peu vos activités et vos enjeux, et que très rarement la configuration de vos locaux ou de votre territoire communal.

Pour vous organiser, il vous est transmis ci-dessous une liste non exhaustive des attentes des pompiers dès qu'ils se présenteront à vous :

- Y a-t-il des personnes en difficulté, des victimes, des personnes ne répondant pas présentes?
- Où se trouve exactement le sinistre, quel est l'accès le plus proche?
- Avez-vous un plan à nous transmettre, quelle est l'origine exacte du sinistre, quels produits sont mis en cause (FDS)?
- Avez-vous un jeu de clés à nous transmettre afin que nous puissions reconnaître la totalité des lieux
- Avez-vous mis à l'arrêt les énergies (eau, gaz, électricité), où se trouvent les éléments de coupure de ces énergies?
- Existe-t-il des enjeux ou des installations à risques?
- Avez-vous un outil de production ou du stockage que vous souhaitez absolument protéger?
- Comment fait-on pour échanger avec le responsable? Avez-vous un numéro à nous donner, avez-vous des radios à nous mettre à notre disposition?

En conclusion, l'aspect structurel d'un plan d'urgence est important pour assurer sa cohérence.

Cependant, sans prise en considération des conseils évoqués dans cet article, il ne répondra jamais à son réel objectif qui est d'assurer le retour à un fonctionnement nominal avec le moins de dégâts possible.

En revanche, son opérationnalité permettra d'éviter la fameuse phrase bien trop souvent entendue après un accident majeur : « Si j'avais su »…

Article écrit par Geoffrey Fillet

Prévention en zone industrielle, ce que les communes/municipalités peuvent faire

5 pistes à l'intention des communes/municipalités pour gérer les risques en zones industrielles sur leur territoire

Prendre contact, échanger avec l'exploitant industriel et visiter le site pour vous approprier des risques existants et prendre connaissance de leur organisation de crise.

Réaliser des exercices de crise en commun en mettant en œuvre concomitamment vos organisations de crise afin d'apprendre à travailler et communiquer ensemble.

Recenser dans votre Plan Communal de Sauvegarde les enjeux situés aux alentours du site industriel et assurer l'information et la bonne évacuation des enjeux humains en cas de crise.

Réaliser des sensibilisations sur les risques majeurs à l'attention de la population communale en partenariat et avec l'intervention de l'industriel.

Inviter les entreprises situées à proximité du site industriel à réaliser leur propre plan d'organisation de mise en sûreté.

Geoffrey Fillet Officier sapeur-pompier volontaire, titulaire d'une licence en « Protection Civile et Sécurité des Populations » ainsi qu'un master en « Gestion globale des Risques Technologiques et Environnementaux », il a effectué un parcours professionnel diversifié dans le domaine de la sécurité et de la gestion des crises, tant dans le secteur public que privé. Sapeur-pompier de Paris et pompier professionnel durant 16 ans, puis chargé Hygiène Sécurité Environnement dans l'industrie, il a ensuite été responsable du service sécurité-sûreté au sein d'un centre hospitalier. Il met aujourd'hui à profit ses 20 années d'expérience ainsi que l'ensemble de ses compétences auprès des différentes organisations afin de développer une réelle « culture de crise ».

> **Il est très rare et même impossible qu'un évènement soit négatif à tous points de vue.**
>
> ***Dalai Lama***

NORME

Renforcer sa résilience face aux risques cyber

Dans un contexte de cybermenaces croissantes, un nouveau guide s'impose comme une référence incontournable pour la gestion des risques cyber au sein des entreprises. Publiée par l'AFNOR, cette norme offre des directives et des bonnes pratiques pour assurer la continuité d'activité et renforcer la résilience en TI.

par Équipe Cyber BRG

Les spécialistes des métiers de la résilience organisationnelle

« SOUS LE PILOTAGE D'AFNOR, PLUS D'UNE QUARANTAINE D'ACTEURS DE TOUTES ORGANISATIONS CONFONDUES PUBLIC OU PRIVES […], ONT MIS EN COMMUN LEURS EXPERIENCES ET LEURS MEILLEURES PRATIQUES EN MATIERE DE CYBER RESILIENCE. LE RESULTAT EST UN GUIDE - AFNOR SPEC CYBER-RESILIENCE, RECONSTRUCTION DU SI ET CONTINUITE D'ACTIVITE METIERS EN CAS DE CYBERATTAQUE PARALYSANTE - COMPORTANT DES LIGNES DIRECTRICES ET RECOMMANDATIONS OPERATIONNELLES POUR ANTICIPER LE TRAITEMENT D'UNE CYBERATTAQUE OU Y FAIRE FACE EN FONCTION DE LA NATURE DE L'ACTIVITE, DE LA MATURITE ET DES MOYENS DE L'ORGANISME QU'IL DEFEND. »

Mais plus concrètement que pouvons-nous trouver dans ce guide ?

De l'identification des risques cyber à l'évaluation de l'impact et de la vulnérabilité

L'AFNOR Spec 2208 offre un cadre précieux aux entreprises pour l'identification des risques cyberpotentiels et l'évaluation de leur impact. En encourageant une analyse approfondie des vulnérabilités des systèmes d'information, cette norme permet de repérer les menaces spécifiques auxquelles une entreprise est exposée. Une fois ces risques identifiés, l'évaluation de leur impact devient essentielle. En comprenant les conséquences potentielles d'une cyberattaque, les entreprises peuvent hiérarchiser les mesures préventives et allouer les ressources nécessaires de manière adéquate. Cette évaluation permet également de mesurer la vulnérabilité de l'entreprise face aux risques cyber et d'orienter les actions de protection à mettre en place.

Ainsi, l'AFNOR Spec 2208 fournit un lien essentiel entre l'identification des risques et l'évaluation de leur impact, permettant aux entreprises de prendre des décisions éclairées pour renforcer leur résilience face aux cybermenaces.

Les spécifications techniques pour la reconstruction du SI, étapes clés du guide

Dans le cadre de la reconstruction du système d'information (SI) après une cyberattaque, l'AFNOR Spec 2208 fournit des recommandations précieuses en matière de spécifications techniques. Cette norme constitue un guide essentiel pour garantir une remise en état efficace du SI tout en renforçant sa résilience face aux risques cyber futurs.

Lors de cette étape critique, la démarche de forensique vise à comprendre l'ampleur de l'attaque, à analyser les méthodes utilisées par les attaquants et à identifier les failles de sécurité exploitées. Les résultats de cette analyse permettent d'orienter les spécifications techniques pour la reconstruction du SI de manière ciblée afin de prendre en compte les architectures réseau, les configurations système et les politiques de sécurité.

Elles doivent être adaptées aux besoins spécifiques de l'entreprise tout en suivant les meilleures pratiques en matière de cybersécurité. Leur mise en œuvre exige une coordination étroite entre les équipes techniques, les experts en sécurité et les métiers impactés. Une communication fluide et la collaboration sont essentielles pour garantir la cohérence et l'efficacité de la reconstruction du SI.

Il est cependant important de noter que la mise en œuvre de ces recommandations peut rencontrer des obstacles tels que la résistance au changement, le manque de ressources et la complexité des processus.

Justement, quels sont ces points de blocage possibles dans la mise en œuvre ?

L'adoption des recommandations peut nécessiter des changements organisationnels et culturels au sein de l'entreprise. La résistance au changement peut provenir de divers acteurs, notamment des collaborateurs qui sont réticents à modifier leurs habitudes de travail. Il est donc essentiel de mettre en place une communication efficace et une sensibilisation continue pour surmonter ces résistances.

La mise en œuvre peut demander également des ressources financières, techniques et humaines conséquentes. Les entreprises peuvent rencontrer des difficultés à allouer les ressources nécessaires pour mettre en place les mesures recommandées. Il est important de réaliser une analyse des coûts et des bénéfices afin de justifier les investissements requis et de mobiliser les ressources adéquates.

La norme aborde des aspects complexes de la continuité d'activité et de la résilience TI. La mise en place des processus recommandés peut être perçue comme complexe et nécessiter une expertise spécifique. Les entreprises peuvent rencontrer des difficultés à comprendre et à mettre en œuvre ces processus de manière efficace. Il est recommandé de se faire accompagner par des professionnels spécialisés comme BRG pour faciliter cette transition.

> “ La résilience informatique est une composante essentielle de la transformation numérique. Les entreprises doivent investir dans des solutions de sécurité avancées et adopter une approche proactive pour se protéger contre les cybermenaces. ”
>
> *Ursula von der Leyen — Présidente de la Commission européenne*

Du coup, comment convaincre les chefs d’entreprise d’appliquer les recommandations de l’AFNOR Spec 2208 ?

La mise en œuvre des recommandations de l’AFNOR Spec 2208 pour renforcer la résilience face aux risques cyber peut sembler complexe pour certains. Cependant, en sensibilisant aux avantages et en mettant en évidence les conséquences d’une cyberattaque, il est possible de les convaincre de l’importance de l’application de ces recommandations.

Convaincre les chefs d’entreprise d’appliquer les recommandations nécessite une approche axée sur les résultats et la mise en évidence des avantages tangibles, tels que la réduction des coûts et la préservation de la réputation.

En comparant l’AFNOR Spec 2208 à d’autres normes internationales, il devient évident que cette norme offre un cadre solide et reconnu pour renforcer la résilience face aux risques cyber.

Il est donc essentiel de présenter ces arguments de manière convaincante afin de favoriser l’adoption de ces recommandations et de garantir une meilleure protection des entreprises contre les cyberattaques.

L’AFNOR Spec 2208 est-elle LA solution ?

Nous ne serions dire si, face aux risques cyber grandissants, l’AFNOR Spec 2208 est la solution, mais il est certain qu’elle offre un cadre structuré et des recommandations essentielles pour renforcer la résilience des TI des entreprises.

En identifiant les risques, en évaluant l’impact et en mettant en place des mesures spécifiques, les entreprises peuvent mieux se préparer contre les cyberattaques et minimiser les perturbations de leurs activités.

Merci à ce groupe de femmes et d’hommes qui ont œuvré à la création de ce guide afin que les entreprises puissent bénéficier d’une démarche proactive et de ses avantages afin d’assurer une meilleure résilience face aux risques cyber.

Article écrit par l’Équipe Cyber BRG

Be Resilient Group : Les spécialistes des métiers de la résilience organisationnelle disposent d’un pôle dédié à la résilience des systèmes d’information nommé « Cyber BRG ». Ce pôle a pour objectif d’aider les entreprises à faire face aux différents risques cyber.

cyber-brg
be resilient group

Desert Overload

2mg, pas plus, risque d'endormissement soudain au-delà. Cette mention sur ma boite de Mélatonine avait conduit le douanier de Doha à me garder une heure à la sortie de l'avion pour en savoir plus. À moins, vu ses coups d'œil indiscrets, qu'il souhaitait passer un moment en bonne compagnie.

Le gros monsieur moustachu me chassa de son bureau avec un signe dédaigneux de la main gauche et je retrouvai les autres passagers de mon vol de Denver qui attendaient leurs bagages depuis une heure quarante. Le tapis était bloqué et des employés asiatiques se démenaient pour nous amener les bagages un à un. Était-ce une conséquence de l'attaque ou de la désorganisation ?

J'avais choisi le cabinet Bullon-Sheritt pour le prestige. Mon MBA de Stanford n'avait rien à voir avec l'informatique, mais mon manager considérait que cette mission pour le gouvernement serait une excellente expérience pour mon premier séjour dans le Golfe.

Mon premier rendez-vous était avec le responsable de la société qui avait déployé le système SmartGrid de la ville deux ans plus tôt. Il me décrit comment ses chefs de projet pakistanais s'étaient fait malmener par les éminences locales.

— Ils nous disaient à chaque réunion : « on veut ce qu'il y a de meilleur, l'argent n'est pas un problème, il faut aller plus vite ». Mais quand il s'agissait de regarder dans le détail, ou décider, il n'y avait plus personne. Le client changeait d'avis à chaque fois qu'un Prince revenait d'une exposition hi-tech. Du coup, nos développeurs ont misé sur GP-Codex pour pouvoir s'ajuster.

Il transpirait à grosses gouttes en secouant la tête de gauche à droite.

— Le système fonctionnait très bien à Doha ; on l'a donc déployé dans plusieurs villes du GCC. Vous connaissez la suite ? dit-il en regardant ses chaussures.

En effet, et c'était bien le problème. Tout ce que ses informaticiens entraient sur cet outil en ligne développé en Israël était analysé à « toutes fins utiles ». Une fois installé, le logiciel du SmartGrid s'est retourné contre plusieurs compagnies électriques de la région le même jour en générant une surcharge qui fit tomber les réseaux… pour la fête de l'Aïd-El-Kébir.

Une dame de la sécurité de Doha Electrics m'expliqua plus tard en pleurant qu'ils avaient bien reçu l'alerte, mais que l'officier de quart n'était pas joignable. La signalisation routière était hors service, engendrant des séries d'accidents. Son beau-fils était décédé.

À Bahreïn, l'incident dans la nouvelle usine de dessalement a conduit l'ONU à intervenir pour acheminer de l'eau potable.

Le plus grave fut, contre toute attente, la perte du système robotisé pour la collecte des déchets de Neom. Les Saoudiens avaient dû évacuer la cité du futur après deux jours, car aucun dispositif alternatif n'était en place. Ce fut un capharnaüm.

Je finis ma mission par un entretien avec Mahir, le fonctionnaire chargé des opérations d'urgence de Doha. Il me dit, bien droit dans son costume traditionnel blanc amidonné, que le soir de l'incident, il s'était empressé de chercher un générateur pour assurer la fête de famille du lendemain, et qu'il n'aurait jamais imaginé que cela dure des semaines, le temps de tout réparer.

— Monsieur, je comprends que l'hôpital central de Doha était submergé, en raison des pannes de climatiseurs. Avez-vous pu consulter leur plan de continuité ?

— Ah, quel malheur ! Non, ce n'était pas mon travail, c'est de la responsabilité du comité de gestion urbaine… ou... du ministère. Vous prendriez bien un Loukoum ? me dit-il en me tendant la boîte avec un beau sourire.

Il n'en restait qu'un.

— La Mecque a été épargnée, divine bénédiction, n'est-ce pas, Mademoiselle Elsa ?

Cela aurait été un désastre pendant les festivités.

Politesse oblige, je ne pouvais nier. La raison qui avait tant mobilisé nos autorités était bien terrestre. Les hackers s'étaient mépris et avaient visé Mecca, la petite ville désertique de Californie.

Auteur : Willard973 - *Willard973 est un cyberpoète en construction, passionné par le futur des industries critiques, les petites erreurs et les grandes débâcles. On dit qu'il a été dans l'armée.*

https://criticalrisks.substack.com/

Gestion de crise : gagner en efficacité opérationnelle avec la digitalisation

Évoluant dans un environnement instable, les organisations doivent anticiper les risques et développer leur résilience. Les communes n'échappent pas à cette obligation de continuité des services qui est l'un des principes fondamentaux du service public. Nous vous proposons de découvrir comment la digitalisation (numérisation) des pratiques révolutionne le domaine de la gestion des crises et de la résilience urbaine.

par Thierry de Ravel

Expertise : gestion de crise et continuité d'activité
Fort d'une double expertise en direction de projets innovants et de conseils en gestion de crise, en 2016, Thierry de Ravel fonde Nanocode, un projet mobilisant ces deux spécialités.

Gérer la continuité des services dans les villes en situation de crise

Les villes et les communes rencontrent différents enjeux liés à la gestion de crise et doivent faire face à des risques de natures multiples :

- Préserver la sécurité des habitants : qu'il s'agisse d'une catastrophe naturelle, d'une pandémie, d'un acte terroriste ou de toute autre situation d'urgence.
- Maintenir les services essentiels : les villes sont responsables de la fourniture de nombreux services essentiels, tels que l'électricité, l'eau potable, les services médicaux, les transports publics, les services d'urgence ou encore la gestion des déchets.
- Préserver les infrastructures critiques comme les réseaux de communication, les systèmes de transport, les hôpitaux...
- Communiquer auprès des citoyens : sur les risques encourus, les mesures prises et les actions à entreprendre en cas de crise.

Les pratiques traditionnelles de gestion de crise dans les communes

En France, les pratiques traditionnelles de gestion de crise dans les mairies sont souvent structurées selon un cadre établi par les plans de gestion de crise nationaux et locaux.

Les mairies élaborent des plans communaux de sauvegarde (PCS) qui définissent les procédures à suivre en cas de crise. Ces plans prennent en compte les risques spécifiques à chaque commune et les ressources mobilisables. Ces données sont souvent en format papier, donc difficilement transportables par les équipes de la ville.

Les mairies mettent en place des cellules de crise municipales lors de la survenance d'un événement critique. Ces cellules regroupent les acteurs clés de la commune, tels que le maire, les services municipaux, la police municipale, les pompiers, les services de santé, etc. Les mairies doivent donc coordonner les activités d'un grand nombre de parties prenantes.

Enfin, les mairies doivent alerter les populations en cas de risques et leur donner des consignes de sécurité : au moyen de sirènes, de messages diffusés via les médias locaux, les réseaux sociaux, les sites internet de la mairie, des applications mobiles dédiées, des panneaux d'affichage, etc.

Émergence de solutions dédiées au pilotage de gestion des alertes et des crises et à la poursuite des activités

En réponse à ces problématiques, des solutions numériques innovantes dédiées à la gestion de crise et à la continuité d'activité émergent. Elles traitent la crise depuis la remontée de l'alerte jusqu'à la sortie de crise et permettent :

- la remontée des alertes à partir de capteurs techniques, des signalements des agents ou des citoyens ;
- la gestion des incidents quotidiens en fonction des astreintes, que ce soit en semaine, la nuit ou le week-end, et selon les différentes professions impliquées (cadre, technique, élu, etc.) ;

5 avantages à l'utilisation d'un outil dédié à la gestion des incidents dans les collectivités :

1-Gérer les plannings d'astreinte des services de la collectivité.

2-Répondre au besoin de mobilité des équipes d'astreinte.

3-Proposer des fiches réflexes interactives permettant de guider le personnel d'astreinte qui n'est pas toujours formé aux situations à risque et de cadrer leur comportement en amont.

4-Fluidifier la communication entre les multiples acteurs, faciliter le reporting aux élus et pouvoir consulter en temps réel l'avancement du traitement des incidents.

5-Assurer la sécurité des données et la continuité de la communication : en cas de cyberattaques, possibilité de communiquer en dehors du système d'information nominal conventionnel (emails et visioconférences sécurisées)

Face à cette multiplicité de risques et d'acteurs, l'enjeu principal va être le déploiement d'une plateforme unique pour adresser toutes les situations anormales

- de bénéficier d'un premier niveau d'assistance à l'aide des fiches réflexes pour guider et faciliter le travail de chacun sur des situations qui ne sont pas toutes maîtrisées ;
- de piloter à distance les équipes devant intervenir par téléphone, messagerie ou système de communication audio/vidéo sécurisé ;
- de produire des rapports concis à l'attention de l'équipe de direction et les élus, dont le maire ;
- d'établir des statistiques pour identifier les situations récurrentes ou les lieux à problème et proposer des améliorations (PDCA).

La solution pour gagner en efficacité : utiliser un outil dédié au traitement des incidents et à la gestion des alertes en amont des crises

Face à cette multiplicité de risques et d'acteurs, l'enjeu principal va être le déploiement d'une plateforme unique pour adresser toutes les situations anormales : du simple incident du quotidien à la crise. Quel que soit le niveau de gravité, l'agent va pouvoir compter sur un outil unique qui va lui permettre de traiter les incidents au jour le jour.

L'efficience côté opérationnel passe indéniablement par la digitalisation des incidents. Cela permet de constituer une base de données des incidents facilement consultable et d'avoir de la visibilité sur le long terme, dans une optique d'amélioration continue. In fine, c'est le service rendu au citoyen qui s'améliore.

En utilisant un seul outil et en impliquant les agents dans la gestion des incidents en amont des crises, on facilite l'adoption de cet outil qui est utilisé au quotidien, on dégage des économies en termes de coût de formation (en évitant d'utiliser plusieurs outils) et surtout, la bascule du mode incident au mode crise se fait plus rapidement, au moment jugé opportun par les émetteurs d'alertes sur le terrain. Ils peuvent escalader très facilement l'alerte auprès de leur cellule de crise si la situation se détériore.

C'est beaucoup plus fluide que la mobilisation traditionnelle d'une cellule de crise en réaction à un événement majeur.

Conclusion

L'investissement initial pour adopter une solution dédiée à la gestion de crise peut sembler être un défi financier pour de nombreuses municipalités, et la résistance au changement est un facteur toujours difficile à appréhender…

Cependant, les avantages de ces outils sont tels qu'ils seront vite incontournables : ils améliorent la réactivité, la communication, la coordination, l'optimisation des ressources, ainsi que le partage des connaissances. Tout cela dans le but de renforcer la capacité des villes à faire face aux crises.

Dans le futur, nous pouvons imaginer l'intégration de l'intelligence artificielle (IA) à ces outils pour anticiper les événements critiques et adapter en temps réel les mesures à prendre.

Cela passera aussi par le développement de capteurs intelligents pour fournir des données en temps réel sur différents paramètres (par exemple, la qualité de l'air, la température, la pression, etc.) et permettre une surveillance continue de l'environnement urbain.

Article écrit par Thierry de Ravel

Les avantages de l'utilisation d'un outil dédié à la gestion de crise par les collectivités à travers la méthode CODAC® en 5 points :

1-Comprendre :

- Bénéficier des données produites par l'astreinte
- Consulter la cartographie tactique (routes bloquées, zones inondées…)
- Accéder à des rapports concis

2-Orienter : Coordonner l'ensemble des acteurs internes et externes mobilisés par la crise

3-Décider : Accéder à des tableaux de bord dédiés au pilotage pour faciliter la prise de décision

4-Agir : Distribuer les actions auprès des parties prenantes et de systèmes applicatifs tiers

5-Communiquer : Communiquer grâce à des fonctionnalités d'envoi de masse et à des bases de contacts préparées à l'avance

Concrètement, la digitalisation des pratiques de gestion de crise révolutionne ce domaine, que ce soit en termes d'accessibilité et de partage de l'information ou encore de retour d'expérience.

Thierry de Ravel : Expert en gestion de crise et continuité d'activité et fort d'une double expertise en direction de projets innovants et de conseils en gestion de crise, en 2016, Thierry de Ravel fonde Nanocode, un projet mobilisant ces deux spécialités.
Contact : Thierry de Ravel, Fondateur et CEO de Nanocode
+33 (0) 6 64 38 12 34

easylience

NANOCODE SAS est une entreprise 100 % française spécialisée dans le développement d'une solution numérique innovante Easylience®, dédiée à la gestion des alertes, des crises et de la continuité d'activité.
https://easylience.com/

Rejoignez-nous sur LinkedIn

Notre page est une ressource précieuse pour ceux qui cherchent à approfondir leur compréhension des crises et de la résilience.

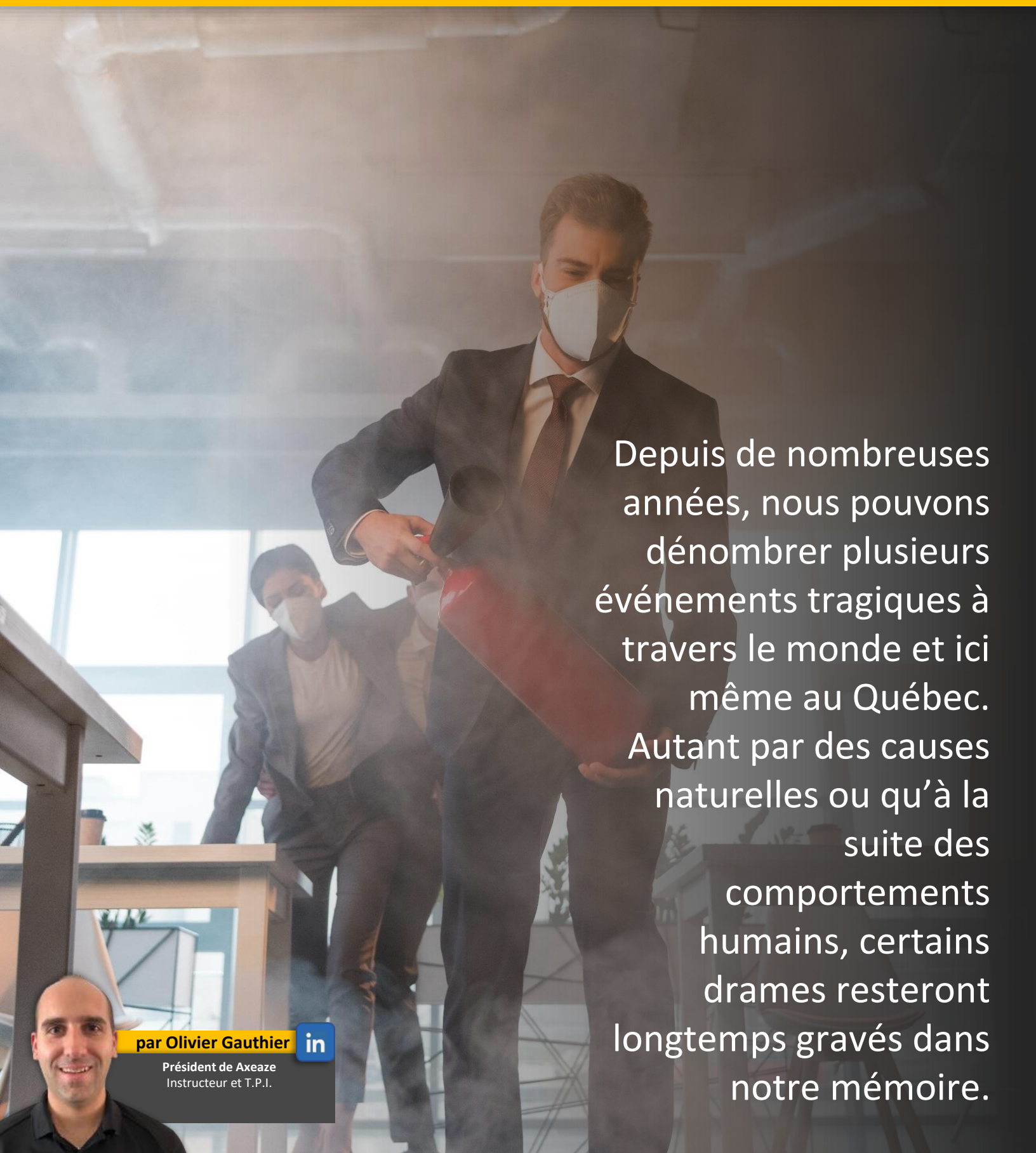
LA SENSIBILISATION DU MOIS

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

Télécharger cette affiche en cliquant ici

ESPACE PUB

L'importance d'un Plan de mesure d'urgence



Depuis de nombreuses années, nous pouvons dénombrer plusieurs événements tragiques à travers le monde et ici même au Québec. Autant par des causes naturelles ou qu'à la suite des comportements humains, certains drames resteront longtemps gravés dans notre mémoire.

par Olivier Gauthier
Président de Axeaze
Instructeur et T.P.I.

Il ne sera malheureusement pas possible d'être parfait et de prévoir toutes les situations, mais tout de même, il faut admettre qu'un plan de mesures d'urgence (PMU) permet d'éliminer beaucoup de risques et de sauver des vies.

Pourquoi avoir un plan de mesures d'urgence?

Que l'on parle de la mise en place de procédures d'urgence en entreprise ou en milieu municipal, il faut comprendre qu'il n'y a aucune raison valable pour omettre une préparation de notre personnel et de nos équipes d'urgence. Le pire peut arriver à tout moment et la sécurité des gens ne devrait jamais être mise de côté.

Le processus d'élaboration d'un plan de mesures d'urgence permet non seulement d'écrire les procédures, mais aussi de réfléchir aux types d'incidents possibles à survenir dans notre secteur. C'est le meilleur moment, en consultation, pour pointer du doigt nos lacunes, particularités et besoins spécifiques. C'est fini le temps où nous pouvions travailler dans nos pantoufles confortables en disant que tout allait bien; c'est maintenant la période idéale pour souligner tous les risques et trouver des solutions avant que le pire ne survienne.

Le plan servira de guide pour le futur et d'outil pédagogique pour les nouveaux arrivés dans une organisation. Une bonne préparation pourra éviter des pertes humaines et matérielles, et même d'éviter une crise. N'oublions pas qu'après un événement d'envergure, il est parfois assez difficile pour des commerces de se relever d'une dure épreuve sans préparation.

De plus, en situation d'urgence, le niveau de stress et la rapidité à laquelle nous devons prendre des décisions sont considérables. Cela facilite grandement les choses lorsqu'une bonne planification a été mise en place d'avance. La gestion de mesures d'urgence n'est pas toujours aussi simple et il faut prévoir d'y consacrer beaucoup de temps avant de voir un résultat efficient.

Les objectifs d'un PMU

Un plan de mesures d'urgence est un plan d'intervention servant de guide pour mieux gérer une situation imprévue.

Le but premier est de prévenir au maximum les accidents et blessures pouvant même causer la mort.

Une bonne prévention passe également par des méthodes d'atténuation des bris et de pertes d'équipements. Ce qui permettra sûrement à une entreprise de recommencer ses activités plus rapidement après un sinistre.

Finalement, l'évaluation externe servira à protéger l'environnement et la population à proximité des lieux.

Dans beaucoup de cas, des victimes auraient pu être épargnées si la préparation à différents scénarios avait été entamée de façon préventive.

À lire aussi
Magazine #1 →

Pratiques (exercices) et réévaluations

Une fois votre plan en place, il est très important de le maintenir à jour chaque année. Le temps passe vite, plusieurs changements dans l'établissement sont faits, sans oublier le roulement dans l'équipe.

C'est pour ces raisons que nous devons prendre une période pour simuler des situations et mettre en action les gens impliqués et y aller sous forme d'essais et erreurs. Souvent, une pratique permet de remettre en question certaines procédures et même de découvrir des éléments manquants dans notre guide.

Autrement dit, je recommande qu'une pratique annuelle soit faite à l'interne et qu'un comité soit créé pour réévaluer le plan au minimum une fois par année également. De plus, lors d'un roulement d'effectif, il est fort pertinent d'y inclure de nouveaux membres pour permettre de jeter un regard différent à nos procédures.

Avez-vous même pensé que d'impliquer les services d'urgence locaux pouvait être un atout dans la planification? Il s'agit d'un travail d'équipe, ne pensez pas que de préparer l'ensemble tout seul sera optimal.

Conclusion

Peut-être que le plan de mesures d'urgence de votre organisation est déjà en place ou en cours de route. Peu importe le rôle que vous avez dans l'organisation, que vous soyez employé, directeur, chef d'équipe, élu municipal ou que vous occupiez tout autre poste, tout le monde mérite d'être mieux protégé et cela commence par une préparation et par l'élaboration d'un plan.

Pour terminer, je tiens à dire que mon équipe et moi sommes disponibles pour vous accompagner dans la planification et l'élaboration de votre plan de mesures d'urgence afin de vous aider à mettre en place un système et des procédures sécuritaires pour votre organisation. Notre expérience, depuis plus de 10 ans dans le domaine de l'urgence, autant médicale que dans l'incendie, nous permet d'apporter des points pertinents et concrets, peu importe votre secteur d'activité.

Article écrit par Olivier Gauthier

Que doit contenir son PMU?

Voici une liste de points nécessaires à la préparation d'un plan de mesures d'urgence. Bien entendu, il n'y a pas de mauvaises questions ou de scénarios non pertinents.

- Liste des scénarios ou situations possibles à survenir
- Liste du personnel d'intervention incluant les coordonnées de chacun
- Rôles et responsabilités de chaque personne
- Plans du bâtiment et localisation des points importants (entrée d'eau, électricité, point de rassemblement, équipements de secours, etc.)
- Liste des ressources externes disponibles
- Procédures en cas d'urgence (médicale, incendie, environnement, agression)
- Document résumé (aide-mémoire) accessible à tous

En fonction du secteur d'activité de l'organisation ou encore des risques et impacts sur la société, il est évident que certains PMU seront plus rapides à mettre en place et beaucoup plus simples. Il est tout de même mieux d'en mettre un peu plus et de résumer si nécessaire.

OLIVIER GAUTHIER
Président, instructeur et TPI
581-705-9011
info@axeaze.ca
www.axeaze.ca

axeaze
Votre solution en prévention

Axeaze est une entreprise Québécoise qui offre une prise en charge complète en matière de premiers soins et sécurité incendie pour aider votre établissement à respecter toutes les normes de sécurité gouvernementales et vous permettre de faire autre chose de votre temps. Vente, location, entretien de trousses de secours, défibrillateurs ou extincteurs portatifs et formation RCR et prévention incendie. Informez-vous sur nos services clé en main adapté sur mesure.

Découvrez la chaîne YouTube Crise et Résilience!

Une plateforme dédiée à vous aider à comprendre et à naviguer à travers des situations difficiles.

Que vous soyez un professionnel cherchant à améliorer votre gestion de crise, ou une personne intéressée par les problématiques de résilience, cette chaîne est faite pour vous.

S'ABONNER ici

À DÉCOUVRIR

Le site Web du
Citoyen prévoyant

Préparation à l'évacuation : Pourquoi nous devons prendre en compte les incidents chimiques

Nous sommes parfois confrontés à des événements qui nous rappellent la pertinence d'une préparation à l'évacuation. Un de ces événements inoubliables est l'accident de train à Mégantic, qui a libéré d'importantes quantités de vapeurs toxiques dans l'atmosphère suite à l'explosion et à la combustion de produits chimiques dangereux. Cela soulève une question cruciale : quel est le meilleur plan d'action si vous habitez à proximité d'une zone à risque ?

Un principe de survie de base est la prudence et l'anticipation : "Faites confiance à vos sens et fuyez". La première règle de la survie est de ne pas être présent lorsque la catastrophe se produit.

Il est vrai que certains pourraient soutenir que l'accident de Mégantic était un incident isolé, un accident de train qui, bien que tragique, reste un événement rare. Cependant, nous vivons dans un monde où l'ordinaire et le prévisible ne sont plus la norme. Les événements sont de plus en plus instables et tumultueux, ce qui change la donne et augmente la probabilité de situations imprévues. En conséquence, il est essentiel de mettre à jour nos stratégies et nos tactiques pour réduire notre vulnérabilité.

Même si vous ne prévoyez pas de vous évader, des circonstances imprévues peuvent vous y contraindre. Il est donc nécessaire de repenser l'évacuation et la relocalisation à la lumière des nouvelles réalités. Les troubles et les dangers peuvent surgir à tout moment et n'importe où. L'histoire regorge d'exemples de personnes qui ont été forcées de fuir leurs maisons par peur d'une menace imminente, qu'elle soit naturelle ou humaine.

En effet, pendant le pic de la pandémie, nous avons été témoins de scènes chaotiques alors que des milliers de personnes tentaient désespérément de quitter des villes comme Paris et Londres avant les confinements annoncés. De plus, nous avons observé des situations dramatiques où les citoyens ukrainiens ont été contraints de fuir leurs villes sous les feux croisés lors de l'invasion russe.

Bien sûr, évacuer ou même anticiper une crise est et restera toujours un scénario extrême et rare - et nous l'espérons tous. Dans 99% des situations, le choix le plus sage est de rester sur place, dans la sécurité de son domicile. Cependant, face à l'instabilité croissante, il est impératif de réévaluer ces stratégies et de considérer toutes les options et toutes les probabilités. Il est crucial de ne pas s'entêter en affirmant : "Je n'évacuerai jamais". Les circonstances peuvent l'exiger, que vous le vouliez ou non.

Que vous viviez en milieu urbain ou rural, il existe divers facteurs de risque à prendre en compte. Pour vous aider, nous vous invitons à visiter ce site qui regorge d'article qui sont plus orientés vers résilience de la personne.

Bonne visite : www.quebecpreppers.com

Surveiller ses actifs en cybersécurité

Cybersécurité – Pourquoi est-il important d'assurer une surveillance continue de ses actifs informatiques par des outils de cybersécurité spécialisés ?

Les logiciels malveillants évoluent constamment et ils représentent des menaces de plus en plus avancées pour les entreprises. Les activités suspectes, les comportements malveillants et les cyberattaques sophistiquées passent maintenant inaperçus par les mesures de sécurité traditionnelles et les départements informatiques.

Lorsqu'une menace est détectée, les entreprises doivent réaliser des réponses rapides et efficaces 24/7 ce qui représente un défi pour celles ne disposant pas de personnel dédié en cybersécurité.

Pour pallier l'évolution rapide de la menace et au manque de ressources humaines spécialisées en cybersécurité dans les entreprises, la surveillance de vos actifs informatiques par des solutions de cybersécurité modernes et avancées s'avère nécessaire. L'industrie de la cybersécurité offre une panoplie de solutions EDR (*Endpoint Detection and Response*), XDR (*Extended Detection and Response*) et MDR(*Managed Detection and Response*). Ces solutions spécialisées permettent d'obtenir une visibilité approfondie des postes, des serveurs, des réseaux informatiques, des raccordements Internet et des tous les dispositifs des entreprises.

Lorsqu'une activité malicieuse est détectée, les solutions EDR, XDR et MDR permettent une réponse rapide et efficace. Elles peuvent automatiser certaines actions comme isoler un poste informatique ou un serveur, désactiver le processus suspect sur un système informatique ou encore bloquer les accès à des ressources critiques comme des serveurs de fichiers. Une réponse rapide et automatique permet de limiter les dommages et d'éviter que la situation ne s'aggrave.

Ces solutions spécialisées permettent une analyse approfondie des activités malicieuses à partir de leurs fonctionnalités d'investigation avancées. Elles fournissent des tableaux de bord et des rapports offrant une visibilité et une gestion centralisée de la cybersécurité d'une entreprise. Les tableaux de bord permettent notamment de prévoir des tendances et de corriger proactivement les vulnérabilités découvertes.

Dans le cas d'une solution MDR, celle-ci est gérée par un fournisseur en cybersécurité et son équipe d'experts qui surveillent en permanence sur les tableaux de bord des outils, les activités, incidents et interviennent au besoin avec les clients. Une solution MDR est notamment fortement recommandée pour les entreprises ne disposant pas d'experts en cybersécurité. Groupe Cyberswat offre notamment un service de surveillance de cybersécurité à ses clients. L'offre de Groupe Cyberswat contribue à renforcer la résilience des entreprises face aux cyberattaques et à protéger les données sensibles de ses clients.

Protéger l'intégrité et la réussite de l'enquête

On anticipe tous d'être victimes d'une cyberattaque en entreprise. Cette réalité n'est pas un secret et dans de nombreux cas, l'attaque provient de l'intérieur. Les motivations derrière ces actes sont variées, allant d'un employé revanchard cherchant à causer des dommages avant de partir, à un employé tenté de vendre des données internes pour arrondir ses fins de mois. Bien que la gestion de crise soit souvent discutée, on parle rarement de la gestion de l'enquête, du moins c'est mon expérience personnelle. Pourtant, cette dernière est cruciale pour identifier les responsables et faciliter le recouvrement auprès des assurances.

Afin de vous aider, voici une liste d'actions à éviter lors d'une enquête cybercriminelle, afin de préserver les preuves :

1. Ne détruisez ni n'altérez les preuves : Il est crucial de ne pas manipuler un ordinateur ayant servi à commettre un crime. Cela équivaudrait à nettoyer une scène de crime, corrompant ainsi les preuves et les rendant inutilisables.

2. Coordonnez-vous avec les autorités compétentes : Dans le cadre d'une enquête, il est essentiel de collaborer avec la police et/ou les enquêteurs. Il est important de les écouter et de ne pas prendre d'initiative sans les consulter, car toute action non sollicitée pourrait avoir les mêmes conséquences que mentionnées précédemment.

3. Assurez-vous d'une communication sécurisée : Lors d'une enquête, tous les échanges doivent être sécurisés entre les participants. Il est possible que le pirate soit encore à l'écoute et profite des moments de faiblesse pour perturber l'enquête.

4. Ne négligez pas la traçabilité et les journaux d'activité : Les journaux d'activités, d'évènements et d'erreurs sont des éléments précieux autant pour les techniciens que pour les responsables, mais également pour la police. Ils peuvent grandement aider une enquête, tandis que leur absence peut compliquer le travail. Prenez donc le temps de les conserver et soyez détaillé dans les logs en entreprise. Considérez cela comme un investissement et une assurance, plutôt qu'une contrainte financière liée à l'espace qu'ils occupent.

En résumé, lors d'une enquête, il est essentiel de préserver les preuves et de veiller à leur sécurité. Contrairement à l'esprit de la startup nation, il est préférable d'adopter une attitude coopérative et à l'écoute envers les autorités compétentes, telles que la police.

Jean-Daniel Genest https://jdgenest.site/about

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

Sécuriser votre AD avant qu'il ne soit trop tard

5 étapes pour la sécurité de l'identité

Les organisations et les analystes reconnaissent maintenant que l'identité est le nouveau périmètre de sécurité, la supervision d'une stratégie de sécurité complète axée sur l'identité est devenue une responsabilité essentielle pour les CISOs

1. Mettre l'accent sur la sécurité axée sur l'identité pour une plus grande résilience opérationnelle : La résilience opérationnelle dépend d'une sécurité solide pour votre infrastructure d'identité, qui est Active Directory (AD) et Azure AD pour 90% des organisations mondiales. La protection de l'Active Directory avant, pendant et après une cyberattaque est essentielle à la résilience opérationnelle.

2. Élaborer une stratégie globale de protection des AD : En raison de la prolifération des attaques contre ad, les analystes, y compris Gartner, appellent maintenant à la sauvegarde et à la récupération spécifiques à AD et à la surveillance régulière pour identifier les vulnérabilités liées à l'identité. Les solutions qui surveillent les attaques AD spécifiques, rétablissent automatiquement les modifications malveillantes apportées à AD et automatisent une récupération complète de la forêt AD sont cruciales pour se protéger contre les cybermenaces actuelles.

3. Obtenez une vue réaliste de votre surface d'attaque d'identité : De nombreuses organisations ont des environnements AD hérités avec des erreurs de configuration qui sont des cibles faciles pour les attaquants. Pour identifier et combler les lacunes de sécurité, les organisations peuvent utiliser des outils puissants tels que Purple Knight, un outil d'évaluation de la sécurité AD gratuit, pour identifier et corriger les vulnérabilités de sécurité.

4. Automatisez la protection de l'identité pour une réponse plus rapide : Les attaques actuelles peuvent se propager à travers le réseau trop rapidement pour une intervention humaine. Pour protéger l'environnement AD, recherchez des solutions qui corrigent automatiquement les modifications malveillantes apportées à l'AD.

5. Effectuer régulièrement des exercices de reprise après sinistre de votre AD : Compte tenu des cyberattaques incessantes sur AD, les organisations devraient se préparer à une cybercatastrophe en ayant un plan de sauvegarde et de récupération spécifique à AD. S'appuyer sur des solutions traditionnelles de protection des données n'est pas suffisant : les sauvegardes traditionnelles incluent à la fois AD et le système d'exploitation sous-jacent, qui peut inclure des logiciels malveillants.

Pour protéger adéquatement votre environnement AD, recherchez une solution de sauvegarde et de récupération AD qui automatise entièrement la récupération de forêt AD à un état exempt de logiciels malveillants et est exempte de dépendances sur des configurations matérielles spécifiques. Voici quelques outils de référence :

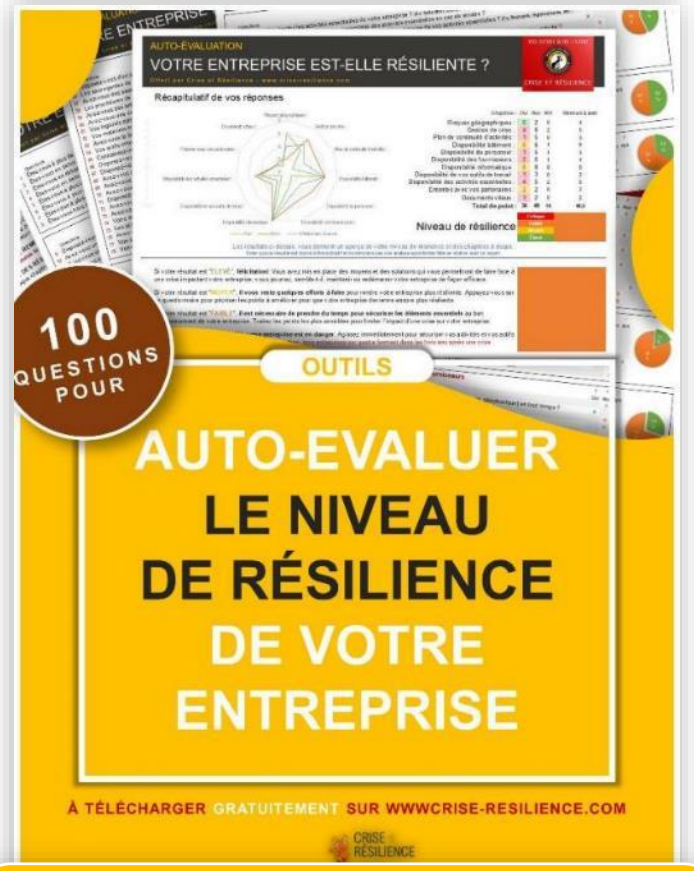
- Semperis - Active Directory - Solutions de sécurité et de récupération AD
- Récupération d'urgence Active Directory | Gestionnaire de récupération (quest.com)
- Administration Cayosoft pour Microsoft Enterprise hybride

Chronique offerte par l'équipe Semperis

Chez Semperis, nous visons à être une force pour le bien. Que voulons-nous dire? L'industrie des ransomwares fait plus que perturber les opérations commerciales. Cette industrie de plusieurs milliards de dollars finance les stupéfiants illégaux, les armes, le terrorisme, la traite des êtres humains et l'exploitation des enfants dans le monde entier. En renforçant la sécurité AD, nous permettons aux organisations de dire « non » aux ransomwares.

L'OUTIL GRATUIT DU MOIS

Découvrez des outils gratuits et pratiques pour préparer la gestion de crise et les plans de continuité des affaires.
Apprenez à anticiper et surmonter les situations difficiles grâce à des ressources simples pour l'évaluation des risques, la planification d'urgence et la communication en situation de crise. Renforcez vos compétences et assurez la résilience de votre entreprise.



Télécharger cet outil en cliquant ici

CONFÉRENCE GRATUITE DU MOIS

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

8 astuces pour bien rater sa gestion de crise

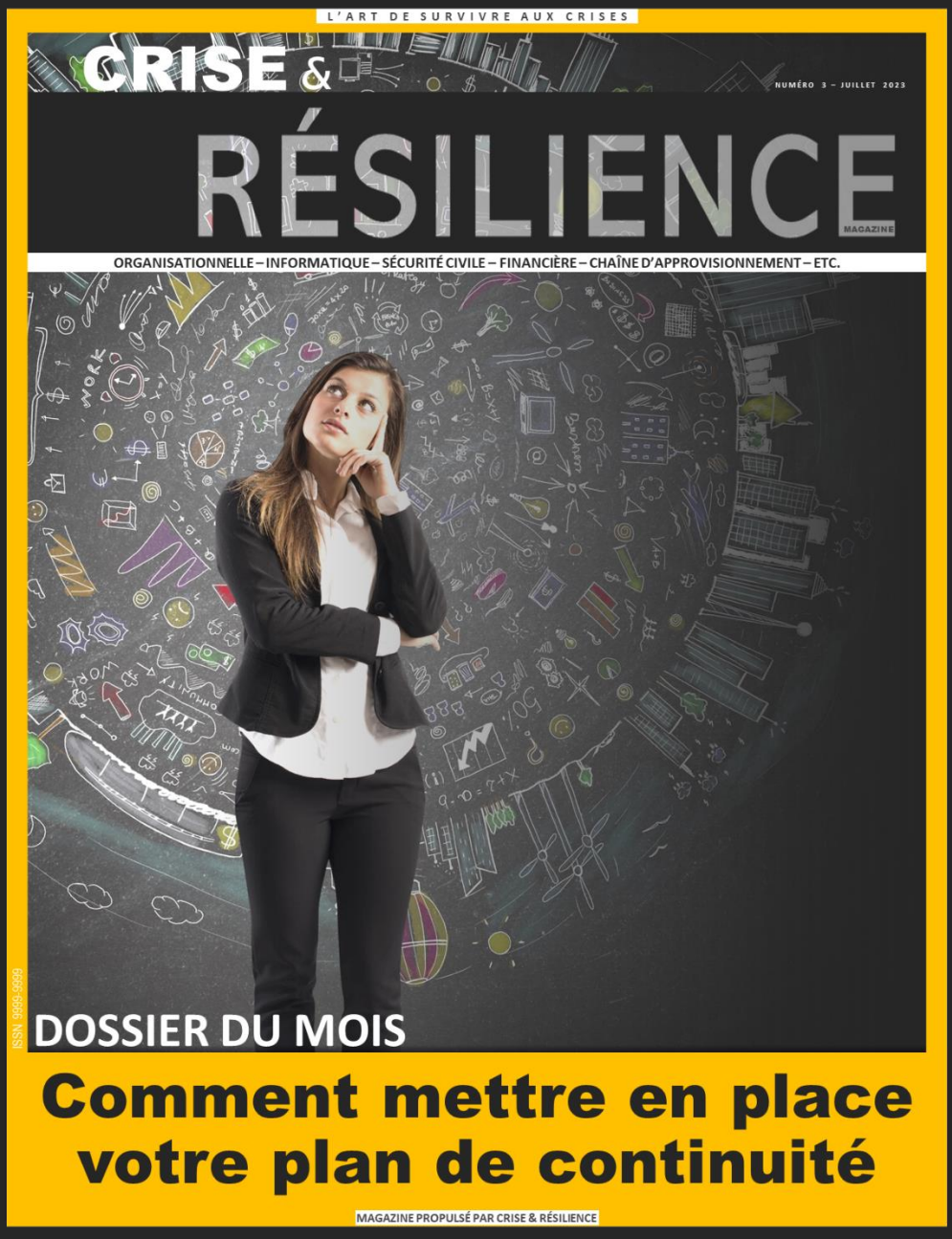
Mesdames et Messieurs, bonjour et bienvenue à cette conférence sur les astuces pour bien rater sa gestion de crise. Si vous êtes ici aujourd'hui, c'est que vous êtes probablement déjà un expert en la matière, ou que vous souhaitez le devenir. Dans tous les cas, vous êtes au bon endroit !

FORMATIONS GRATUITES

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

NE RATEZ PAS LE PROCHAIN MAGAZINE

Prochain numéro le 2 Octobre 2023



Abonnez-vous

pour recevoir le prochain magazine

www.Crise-Resilience.com/magazine