L'ART DE SURVIVRE AUX CRISES

CRISE & RÉSILIENCE MAGAZINE

NUMÉRO 1 – JANVIER 2023

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

2 FORMATIONS CYBERCRISE À GAGNER
Valeur de chaque formation 2 997 $

27 PISTES DE SOLUTIONS
POUR SURVIVRE À UN *BLACKOUT* INFORMATIQUE

8 STRATÉGIES POUR PRÉPARER VOTRE ENTREPRISE À LA RÉCESSION

72 HEURES POUR SURVIVRE AVANT L'ARRIVÉE DES SECOURS

OUTIL DU MOIS:
15 ACTIONS À PRENDRE LORS D'UNE CYBERATTAQUE

MERCI À
EMMANUELLE HERVÉ,
QUI EST LA MARRAINE
DE CE PREMIER MAGAZINE

LA COMMUNICATION DE CRISE…
UTILE OU FUTILE?

DOSSIER DU MOIS

Blackout informatique

ISSN 9999-9999

MAGAZINE PRODUIT PAR CRISE & RÉSILIENCE

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

UN MOT SUR LA MARRAINE DE CE NUMÉRO

Emmanuelle Hervé
Présidente fondatrice d'EH&A, cabinet spécialisé en gestion et communication de crise.

Experte internationalement reconnue en gestion de crise et en communication sensible et de crise, Emmanuelle accompagne organisations et dirigeants depuis plus de quinze ans.

Ingénieure de formation, Emmanuelle parcourt le monde et enchaîne les expatriations.

Sa carrière professionnelle s'amorce en Inde en 1994. Ensuite, elle s'installe à Beyrouth pour gérer un projet industriel, puis rejoint le groupe de chimie américain DuPont de Nemours en 1998, pour qui elle développe le marché MENA. Sa vie se partage alors entre la Jordanie, l'Égypte, la Turquie, l'Afrique, les Émirats arabes unis, l'Iran et les États-Unis.

De retour en France en 2006, forte d'une fine connaissance des pays où elle a vécu et parfois traversé des situations de tension géopolitique, Emmanuelle rejoint le cabinet MGVM dans le domaine de la gestion de crise. Depuis plus de quinze ans, elle accompagne les entreprises dans la préparation et la gestion de crise. Elle les aide à élaborer une stratégie à long terme afin de résoudre leurs crises.

Son cabinet EH&A Consulting est classé « incontournable » par le magazine « Les Décideurs » depuis 2020.

Emmanuelle est également engagée au sein de nombreuses instances:

- Présidente de la commission AFNOR et du groupe de travail international ISO sur la e-réputation.
- Membre active du CIAN (Conseil français des investisseurs en Afrique)
- Experte assermentée de l'ONUDI (Organisation des Nations Unies pour le développement industriel)
- Experte Communication de crise pour différents médias
- Auditrice IHEDN (Institut des Hautes Études de Défense Nationale) session nationale 2021-2022

Depuis 2018, Emmanuelle est Officier de réserve de la Marine nationale. Cet engagement citoyen l'anime à titre personnel et lui permet, à titre professionnel, à l'augmentation de la porosité entre les mondes civil et militaire et au rayonnement de la Marine.

Emmanuelle est une vraie professionnelle de la gestion de crise avec un excellent palmarès qu'elle partage avec passion, enthousiasme et pragmatisme.

sommaire

Numéro 1 – JANVIER 2023

Rejoignez-nous sur **LinkedIn**

ÉDITO DE LA RÉDACTION

De plus en plus, nous traversons des événements qui mettent à l'épreuve notre résilience. Nous avons tous été confrontés à des difficultés et des incertitudes inédites pour nos générations. Malgré ces défis, nous avons continué à avancer, à trouver de nouvelles solutions et à nous adapter à un monde en constante évolution.

La résilience est une qualité vitale pour affronter les crises et les défis à venir. Elle nous permettra de surmonter les obstacles et de trouver des moyens de survivre. Alors que nous entamons une nouvelle année remplie de nouveaux défis économiques, énergétiques, météorologiques, cybernétiques et géopolitiques, préparons-nous à maintenir à flot nos entreprises dans une tempête qui s'annonce brutale.

Avec ce premier numéro de notre magazine, nous voulons partager avec vous les clés, les stratégies, les expertises qui, nous l'espérons, vous permettront de faire face aux défis de 2023. Dans les articles, vous découvrirez des techniques, des solutions, des outils et des guides inspirants accompagnés de conseils pratiques pour développer votre propre résilience.

Je tiens à exprimer ma plus sincère gratitude envers toutes les personnes qui ont contribué au lancement de ce premier magazine et qui ont placé leur confiance en moi. Merci!

Alexandre Fournier

Rédacteurs ayant participé à ce magazine par ordre alphabétique: Alexandre Fournier, Cyrille Augustin Molemb Beal, Emmanuelle Hervé, Guillaume Carr, Jean-Philippe Racine, Karine Maréchal-Richard, Nicolas-Loïc Fortin, Olivier Gauthier, Stéphanie Moreau.

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

LA RÉSILIENCE ORGANI-QUOI?

La résilience organisationnelle est la capacité d'une entreprise à faire face aux difficultés et aux défis, qu'ils soient internes ou externes, à continuer à fonctionner de manière efficace et à atteindre ses objectifs.

Elle est devenue une qualité cruciale pour les entreprises de toutes tailles et de tous secteurs, qui doivent faire face à un monde en constante évolution et à des perturbations de plus en plus fréquentes.

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.

La résilience organisationnelle peut être vue comme une combinaison de facteurs internes et externes qui permettent à l'entreprise de se remettre rapidement d'un choc ou d'un obstacle, et de continuer à prospérer. Parmi les facteurs internes, on peut citer la culture d'entreprise, la structure de l'organisation, les processus décisionnels, les ressources humaines et financières et les systèmes de gestion.

Les facteurs externes comprennent les changements de l'environnement économique, technologique et réglementaire, ainsi que les événements imprévus tels que les catastrophes naturelles ou les pandémies.

Pour développer la résilience organisationnelle, il est important que les entreprises mettent en place des stratégies et des plans de continuité des activités qui leur permettent de faire face aux perturbations et de continuer à fonctionner de manière efficace. Cela peut inclure la mise en place de processus de gestion de crise, la formation du personnel aux techniques de gestion du stress et de gestion d'équipe, et la mise en place de plans de secours pour les situations d'urgence.

En outre, il est important que les entreprises soient flexibles et en mesure de s'ajuster aux changements de l'environnement. Cela peut nécessiter d'investir dans la technologie et l'innovation, ou encore de créer des canaux de communication efficaces avec les principales parties prenantes – clients, fournisseurs et employés.

La résilience organisationnelle est également liée à la culture d'entreprise et à la capacité de l'organisation à maintenir une vision à long terme et à s'adapter à l'incertitude.

Pour y parvenir, il est important que les dirigeants de l'entreprise soient des leaders forts et visionnaires, capables de guider l'entreprise dans les moments difficiles et de maintenir la motivation et le moral de l'équipe.

Peu importe comment vous définissez le succès, vous devrez être résilient, fort, authentique et agile pour y arriver.

Joanie Connell

La résilience organisationnelle est cruciale pour la survie et la réussite à long terme de l'entreprise, elle permet également aux employés de se sentir en sécurité et de travailler efficacement même dans les moments difficiles.

3 Bénéfices

Capacité à faire face aux perturbations et à s'adapter aux changements: une organisation résiliente est en mesure de gérer efficacement les crises et les perturbations, tout en continuant à fonctionner de manière efficace et à atteindre ses objectifs.

Meilleure gestion des risques: une organisation résiliente est mieux équipée pour identifier et gérer les risques potentiels, ce qui peut réduire les pertes financières et les dommages potentiels.

Avantage concurrentiel : Les organisations résilientes ont tendance à être plus flexibles et mieux adaptées aux changements de marché, ce qui leur permet de réagir plus rapidement et plus efficacement aux opportunités et aux menaces concurrentielles. Cela les met en avantage face à des organisations moins résilientes et peut les aider à se démarquer et à maintenir leur avantage concurrentiel sur le marché.

Alexandre Fournier

12 facteurs de succès de la résilience organisationnelle

1. **Vision claire et objectifs stratégiques.** Une organisation qui a une vision claire et des objectifs stratégiques bien définis est mieux préparée pour faire face aux défis et aux perturbations.
2. **Leadership fort.** Un leadership fort est essentiel pour soutenir l'organisation et la guider pendant les périodes difficiles.
3. **Culture de l'innovation.** Une culture de l'innovation qui encourage l'exploration de nouvelles idées et la prise de risques peut aider l'organisation à s'ajuster aux changements.
4. **Communication efficace.** Une communication efficace est cruciale pour s'assurer que tous les membres de l'organisation sont informés et impliqués dans les décisions et les changements.
5. **Collaboration et travail d'équipe.** La collaboration et le travail d'équipe sont des éléments clés de la résilience organisationnelle, car ils permettent de mobiliser les ressources et les compétences de l'ensemble de l'organisation pour faire face aux difficultés.
6. **Flexibilité et adaptabilité.** Une organisation qui est flexible et adaptable est plus à même de s'adapter aux changements et de trouver de nouvelles opportunités.
7. **Gestion des ressources.** Une gestion efficace des ressources, y compris les ressources financières, humaines et matérielles, peut aider l'organisation à maintenir son fonctionnement pendant les périodes difficiles.
8. **Gestion du changement.** Une gestion efficace du changement peut aider l'organisation à naviguer de manière fluide et à réussir dans un environnement en constante évolution.
9. **Gestion des risques.** Une gestion efficace des risques peut aider l'organisation à identifier et à gérer les risques qui pourraient perturber son fonctionnement.
10. **Préparation aux situations d'urgence.** Une préparation adéquate aux situations d'urgence peut aider l'organisation à réagir rapidement et efficacement lorsqu'une crise survient.
11. **Réseaux de soutien.** Des réseaux de soutien externes tels que des partenaires, des fournisseurs et des clients peuvent être un atout précieux pour l'organisation pendant les périodes difficiles.
12. **Engagement des employés.** Un engagement fort et positif des employés peut aider l'organisation.

Évaluer votre résilience en cliquant ici

LA COMMUNICATION DE CRISE, UTILE OU FUTILE?

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.

INTERVIEW

Emmanuelle Hervé

Présidente fondatrice d'EH&A, cabinet spécialisé en gestion et communication de crise

Dans notre métier, personne n'est à l'abri d'un événement qui pourrait mettre en danger la survie de notre entreprise.

Et lorsque cet événement survient, il faudra mettre sur pied un processus de gestion de crise et un protocole de communication de crise.

La communication, c'est quoi?

La communication de crise est aussi importante que la gestion de crise. La gestion de crise va vous permettre de gérer de façon organisée la crise qui survient et d'effectuer un retour à la normale plus rapide. La communication de crise vous indique comment communiquer avec les différentes parties prenantes de votre entreprise (les victimes, vos clients, vos actionnaires, etc.). La communication en cas de crise est très importante, car elle permet:

- d'écarter les rumeurs autour de ladite crise; même si l'entreprise ne communique pas, l'histoire va se savoir. Des personnes lambda qui ne connaissent pas les réalités de votre métier pourraient propager une histoire très approximative de celle qui vous arrive réellement. Nous savons tous que les gens ont tendance à déformer la réalité pour attirer l'attention. Le boycottage de votre entreprise pourrait être une conséquence directe de ces rumeurs;
- de conserver de bonnes relations entre vos partenaires et vous. Si vous communiquez avec vos parties prenantes, les relations resteront solides. En effet, si vos partenaires prennent connaissance de la situation à travers les médias, ça risquerait de les contrarier. Il est donc nécessaire, voire indispensable, de les mettre au courant avant toute chose.

Généralement, la difficulté rencontrée est que l'organe chargé de faire la communication de crise est le même que l'organe chargé de faire la communication de l'entreprise. Or, il faut savoir que ceux qui font de la communication marketing ne font pas forcément de la communication de crise: il s'agit de deux domaines bien différents.

« La communication est une science difficile. Ce n'est pas une science exacte. Ça s'apprend et ça se cultive. »

De Jean-Luc Lagardère

Pour une communication de crise réussie, vous devez appliquer le système E.T.A

Empathie. S'il y a eu des victimes physiques, des gens qui ont eu peur, etc., faites preuve d'empathie, de compréhension. Traitez vos clients comme des personnes et non comme des consommateurs. Traitez vos partenaires comme des membres fondamentaux de votre entreprise. Il est absolument fondamental que vous vous y preniez avec douceur et patience – c'est peut-être la partie la plus délicate de la communication de crise.

Transparence. Impliquez vos partenaires et vos clients dans le processus de gestion de crise. Ne laissez aucune zone d'ombre. Tenez-les informés de l'évolution des enquêtes, par exemple. Vous devez éviter de minimiser l'importance des informations à fournir à vos partenaires. Bien sûr, la transparence ne signifie pas de tout dire; il y a un certain niveau de secret à garder dans le cadre de la crise. C'est un vrai travail de distinguer ce qui relève de l'information à garder pour vous et ce qui relève de l'information à divulguer aux parties prenantes. En fait, la transparence, c'est aussi d'expliquer pourquoi vous ne pouvez pas divulguer certaines informations.

Actions. Dites à vos parties prenantes tout ce que vous comptez faire pour gérer la crise. Leur dire que tout va bien ne va pas les rassurer. Vous devez leur présenter votre plan d'action pour qu'ils soient en confiance.

Enfin, vous devez démontrer votre engagement. Montrez à vos partenaires que vous êtes engagés à 100 % dans la gestion de la crise, tant par la parole et par les actes.

EMPATHIE
TRANSPARENCE
ACTIONS

VOICI QUELQUES FACTEURS DE RÉUSSITE QUI FAVORISERONT UNE BONNE COMMUNICATION DE CRISE

- **Évitez le déni.** Vous devez absolument éviter de vous convaincre que tout va bien. Vous devez prendre en considération la situation et la traiter comme une crise qu'il vous faudra gérer.
- **Ne cherchez pas de boucs émissaires.** Ne rejetez pas les fautes sur les autres. Vous devez assumer vos actes et vos positions par rapport à la crise.
- **Ayez un plan de communication personnalisé.** Ne gérez pas la crise comme les autres entreprises le font ou l'ont fait. Chaque entreprise est unique et doit avoir son propre protocole de communication de crise.
- **Ne tombez pas dans la victimisation.** Certes, vous faites face à une crise, mais les premiers responsables devant la loi, c'est d'abord vous.
- **Ne faites pas preuve d'arrogance.** Acceptez toute l'aide qui se présente à vous, quelle qu'elle soit. Votre comportement reflète la façon dont vous gérez vos clients.
- **Ne tombez pas dans les griffes de la stratégie juridique.** Bien que nécessaire, cette stratégie est trop agressive. Oui, les juristes doivent faire leur travail, mais ce n'est pas la base de votre communication de crise. Ne laissez pas vos avocats communiquer pour vous dans le cadre de la crise.

Comment gérer les médias?

Les médias classiques

Il faut savoir que l'objectif d'un journaliste, c'est de vendre. Si vous avez bien communiqué, bien appliqué le système E.T.A, le journaliste écrira des informations justes et véridiques. Par contre, si vous négligez la communication, le journaliste va chercher des sources par lui-même. Vous conviendrez avec moi que la plupart des sources vers lesquelles il risque de se rediriger proviendront de vos détracteurs, qui chercheront à déformer la vérité pour nuire à votre entreprise. Résultat: des articles remplis de fausses informations seront mis en vente. Il ne faut surtout pas critiquer les journalistes, qui sont payés pour produire des contenus vendables.

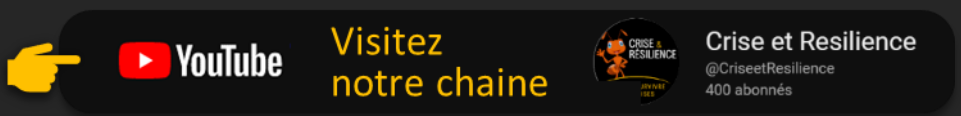
Les réseaux sociaux

Vous devez savoir que sur les réseaux sociaux, il y a une sorte de paresse intellectuelle: les gens ne cherchent pas trop à distinguer le vrai du faux. Les réseaux sociaux sont remplis de personnes qui se font elles-mêmes leur opinion, ce qui peut affecter votre entreprise. Vous devez inclure cela dans votre processus de communication de crise. C'est important, car les gens qui véhiculent des mensonges pensent peut-être réellement que c'est vrai. À vous de jeter une lumière sur ce qui se dit de faux sur la crise.

En conclusion, nous vous conseillons de ne pas attendre d'être confronté à une crise pour mettre sur pied une cellule de gestion de crise. Vous devez le faire le plus tôt possible dans le but de prévoir les différentes crises qui pourraient survenir.

Propos recueillis par Alexandre Fournier.

Interview Parole d'experts



L'ANTICIPATION, LE CŒUR DE LA GESTION DE CRISE

En gestion de crise, l'anticipation fait référence à la capacité d'imagination de scénarios défavorables sur l'évolution d'une situation.

Anticiper l'évolution d'une crise grâce à la construction des scénarios en considérant toutes les dimensions de celle-ci

(RH, juridique, financier, opérationnel, réputationnel, IT, etc.)

permet de construire un plan d'action pertinent.

Par Emmanuelle Hervé

Présidente fondatrice d'EH&A,
cabinet spécialisé en gestion et communication de crise.

« Prendre les devants sur une situation future pour limiter les impacts négatifs »

En gestion de crise, l'anticipation fait référence à la capacité d'imagination de scénarios défavorables sur l'évolution d'une situation. Anticiper l'évolution d'une crise grâce à la construction des scénarios en considérant toutes les dimensions de celle-ci (RH, juridique, financier, opérationnel, réputationnel, IT, etc.) permet de construire un plan d'action pertinent.

Dans notre monde volatile, incertain, complexe et ambigu, être en mesure « d'imaginer des scénarios futurs » est une qualité recherchée par les organisations pour faire face aux crises. Cette qualité s'acquiert grâce à de la méthode, au partage de la vision, au suivi des temporalités de la crise et à l'entraînement.

Dans la gestion de crise, l'incertitude fait partie du lot de tous les jours. Cependant, nous pouvons tenter de prendre les devants en anticipant les risques. L'anticipation est le seul moyen de garder une longueur d'avance et d'imaginer comment une situation peut empirer. Elle permet de garder une marge d'erreur, un temps pour se préparer, cartographier les parties prenantes, les dangers, et ce, dont on aura besoin pour remédier à la crise.

L'importance de l'anticipation réside principalement dans la préparation. En effet, de nombreux chefs d'entreprises ne voient pas les crises arriver. Il est parfois difficile de voir au-delà et d'imaginer que quelque chose pourrait mal tourner. Dans ces situations, les conséquences peuvent être catastrophiques:

- Mauvaise gestion de la crise.
- Communication bancale
- Manque de coordination entre les membres de l'équipe
- Enregistrement imprécis des actions prises, des informations prises par manque d'anticipation des outils nécessaires: logiciels dédiés à la gestion de crise, mind mapping, white board…

4 clés pour développer sa capacité d'anticipation:

Afin d'éviter ces conséquences, il y a 4 grandes thématiques à appliquer qui permettent de développer la capacité d'anticipation:

Organiser une veille active: celle-ci permet de se tenir informé des évolutions de l'entreprise, de son environnement, des signaux faibles… Afin d'avoir un coup d'avance en permanence.

Définir un plan de crise: il permet de savoir ce qu'est une crise, comment s'organiser en interne pour affronter la situation, de savoir quels sont les membres de sa cellule, d'identifier les scénarios défavorables pour adapter les prises de décisions.

Se former et s'entraîner pour réagir aux imprévus avec plus d'agilité: formations méthodologiques, media training, exercices pratiques, simulations… ce panel permettra aux membres de la cellule de crise et aux porte-parole de développer les réflexes, et l'agilité nécessaire quand une crise survient.

Maîtriser et savoir manier la communication de crise: la communication de crise est un atout important de la gestion de crise, car elle vient accompagner le processus et les actions mis en place par la cellule de crise pour les diffuser vers les parties prenantes avec le bon timing. Bien utilisée, elle permet d'éviter les sur-crises qui surviennent parfois même si la gestion opérationnelle de la crise a été bien faite.

« Anticiper les crises, c'est d'abord fédérer les énergies.

Il s'agit ainsi d'identifier les profils et d'associer les personnalités réellement adaptés aux fonctions de la cellule de crise. »

L'entreprise doit penser à toutes les situations susceptibles de provoquer une crise et de s'y préparer dans le but d'agir plutôt que de réagir, anticiper plutôt que subir. Concrètement, anticiper permet d'être capable de se mobiliser sans délai en cas de crise à chaud et les bonnes pratiques à appliquer durant les exercices de crise « à froid ».

C'est pourquoi se préparer à gérer d'éventuelles crises est primordial pour ne pas être désarmé lorsqu'elles se produisent. Mesurer les risques, élaborer des plans d'anticipation, planifier des exercices d'entrainements, sont des éléments essentiels pour diminuer les conséquences éventuelles de la crise. L'ajustement des procédures, des méthodes et des outils ou la mise en place de ceux manquant ainsi que la formation et l'entraînement des équipes doivent permettre à l'organisation de mieux anticiper et se préparer pour des crises futures.

Emmanuelle Hervé

Les crises font désormais partie de la vie d'une entreprise et savoir les anticiper et y répondre n'est plus une expertise facultative.

Notre métier est de protéger votre réputation, de préserver la valeur de votre entreprise et d'assurer ses futures opportunités.

Leader dans la gestion de crise, la communication sensible, la prévention des risques et la continuité d'activité, EH&A est reconnue en France, en Europe, au Moyen-Orient et en Afrique.

Notre équipe multidisciplinaire vous accompagne au quotidien avec pragmatisme et méthode: planification de scénarios, gestion de la réputation, gestion de la relation avec les médias et les parties prenantes, continuité d'activité. Notre écosystème vous apporte également son expertise dans les domaines de la sécurité, santé et environnement, accompagnement psychologique, protection des biens et des personnes, surveillance des réseaux sociaux et des journalistes.

L'empathie, l'humilité, l'intégrité et la responsabilité sont les piliers sur lesquels nous avons bâti notre réputation.

Pendant une crise, une équipe réactive se tiendra à vos côtés et vous aidera à organiser votre réponse, mobiliser vos collaborateurs et élaborer votre stratégie de gestion de crise. Nous garantissons des interventions rapides et discrètes.

L'OUTIL DU MOIS

Évaluer la résilience de votre entreprise.

La résilience d'une entreprise est sa capacité à faire face aux défis et à maintenir ses activités malgré les difficultés rencontrées. L'évaluation de cette capacité est donc essentielle pour s'assurer que l'entreprise est en mesure de gérer les aléas de l'environnement dans lequel elle évolue.

Pour savoir où se situe votre entreprise, vous pouvez utiliser l'outil « **Auto-évaluer le niveau de résilience de votre entreprise** ». Cet outil vous permettra de mesurer différents aspects, notamment vos risques géographiques, la maturité de vos plans de gestion de crise et de continuité des activités, la disponibilité du vos bâtiments et installations, de vos employés, de vos fournisseurs, de votre système informatique, de vos outils de production, de vos activités essentielles ou encore de vos ententes partenariales et autres documents essentiels.

Télécharger cet outil en cliquant ici

Vous souhaitez proposer un outil? Contactez-nous: info@crise-resilience.com.

LA CONTINUITÉ DES AFFAIRES UN PROJET VITAL POUR LES ENTREPRISES

Voici une histoire qui n'arrive pas qu'aux autres…

En lisant le journal, votre directeur apprend que l'entreprise de l'un de ses amis est en grande difficulté. Elle fait face à une crise majeure, causée par une inondation.

Dans l'article, le dirigeant principal de la société en question affirme:

« J'aurais dû m'organiser pour anticiper cette crise! »

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.

Forcément, cette histoire a marqué votre directeur et il décide d'agir pour se prémunir d'un sinistre et, surtout, être organisé en cas de crise majeure. Il ne souhaite pas perdre son entreprise en plus de subir un sinistre.

Après plusieurs recherches, il conclut qu'il faut mettre en place un plan de continuité des affaires (PCA).

Ce plan permettra à l'entreprise d'être organisée pour faire face à un sinistre, de connaître ses activités essentielles et de les maintenir afin de respecter ses engagements envers ses clients en cas d'interruption de service.

Mieux vaut prévenir…

Lorsque l'on parle de résilience et de sinistres, plusieurs exemples d'événements non désirés et lourds de conséquences pour les entreprises nous viennent à l'esprit: inondations, pannes majeures, attaques logicielles, rançons, perte d'environnements informatiques, etc.

Ces sinistres se traduisent toujours par des pertes opérationnelles, parfois très importantes, qui peuvent aller jusqu'à la fermeture définitive de l'entreprise.

« La continuité des activités est la clé pour assurer la survie de votre entreprise dans les situations de crise. »

Le plan de continuité des affaires (PCA) permet à l'entreprise de se préparer et de connaître à l'avance toutes les actions à réaliser en cas de sinistre, ce qui lui permet d'en réduire les impacts.

Vous êtes l'élu, félicitations!

Le directeur vous informe que vous allez être nommé responsable du PCA.

Ce choix apparaît d'autant plus pertinent que vous êtes déjà dans l'entreprise depuis plusieurs années. Vous connaissez bien son fonctionnement et, surtout, vous vous êtes démarqué en gérant plusieurs projets d'envergure complexes.

Vos capacités de gestionnaire de projet sont jugées essentielles à la conduite de cet important dossier.

OUPS!

Quoi faire?
Par où commencer?
Qu'est-ce qui est prioritaire?
Autant de questions qui font très mal si on est mal ou pas préparé!

Suivant les bonnes pratiques du PMBOK[(1)], la première étape du projet consiste à nommer un responsable du plan de continuité.

La première tâche de cette personne, avant de démarrer le projet, est de se documenter et de chercher à répondre aux questions suivantes…

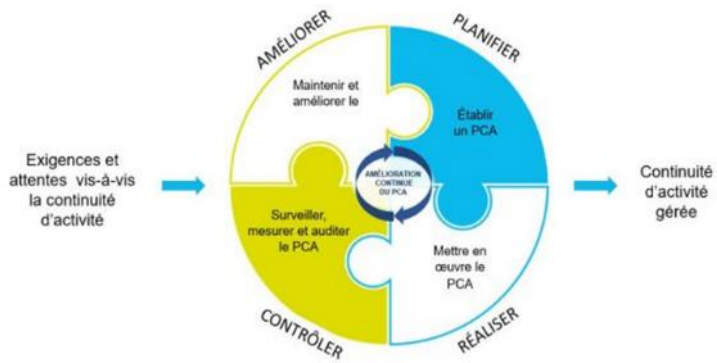
- Comment met-on en place un plan de continuité?
- Quelle doit être sa portée considérant sa nature transversale?
- Quelles sont les bonnes pratiques à appliquer pour réussir un tel projet?
- Qui doit y participer? Quelle taille doit avoir l'équipe?
- Comment planifie-t-on un tel projet?
- Etc.

[(1)]Project Management Body of Knowledge

DÉFINIR, METTRE EN ŒUVRE, CONTRÔLER, MAINTENIR ET AMÉLIORER UN PCA

Après quelques recherches, on se rend vite compte qu'une démarche de continuité implique autant le domaine des affaires que celui de l'informatique.

C'est pourquoi vous prendrez bien soin d'inclure dans votre équipe des représentants des deux groupes. Pour faciliter la conception d'un PCA, il est aussi fortement recommandé d'utiliser un modèle conceptuel qui vous assure de couvrir tous les angles et exigences qui découlent d'un tel projet.



Pour définir, mettre en œuvre, contrôler, maintenir et améliorer un PCA, la norme ISO 22 301 applique le cycle PDCA (Plan, Do, Check et Act) ou roue de Deming.

PAS DE PANIQUE!

Voici quelques éléments pour bien démarrer.

Comme illustré à la page précédente, la démarche comporte quatre grandes étapes qui contribuent à construire votre PCA:

- Planifier
- Réaliser
- Contrôler
- Améliorer

Comme dans tous projets, il faut commencer par une étape de planification, qui incorpore les exigences et les attentes vis-à-vis de la continuité d'activité à la démarche et qui précise les autres éléments fondamentaux à considérer pour la réalisation du PCA.

Vous allez constater qu'il y a beaucoup de points communs entre les bonnes pratiques de gestion de projet et la mise en place d'un PCA.

En effet, avant d'avoir un PCA opérationnel, il faut d'abord faire autoriser le projet par la direction et l'inscrire ensuite au portefeuille de projets de l'entreprise.

Après quoi, il faut produire un plan de projet.

Pour vous y aider, voici les principaux éléments que l'on retrouve généralement dans un PCA.

1 Définir le contexte

Qu'est-ce qui motive l'entreprise à mettre en place un PCA? Est-ce que votre entreprise appartient à une branche d'activité qui oblige toutes les entreprises de cette même branche à mettre en place un PCA? (par exemple, Bâle III – les organisations de tutelle obligent toutes les banques à mettre en place un PCA). Est-ce pour répondre à un besoin exprimé par la direction pour démontrer à ses clients et à ses investisseurs que, quoi qu'il arrive, l'entreprise saura faire face à une crise? Etc.

2 Définir les objectifs

Pourquoi mettre en place un PCA? Quelles sont les conséquences pour l'entreprise si elle ne remplit pas sa mission? Y a-t-il une perte de revenus, une atteinte à la réputation, un impact sur la santé et la sécurité des personnes, des dépenses supplémentaires, etc.? En répondant à ces questions, vous définirez les objectifs du projet.

3 Définir le portée

Quels sont les produits et services, les sites, les fonctions, les processus et les activités, les parties prenantes qui seront couverts par le PCA? Lorsque l'on parle de produits ou de services, cela couvre implicitement tous les flux des produits et des informations qui vont de l'achat des matières premières (fournisseurs) jusqu'à la livraison des produits finis aux consommateurs (clients). De plus, comme dans tous projets, il ne faut pas oublier de nommer et de documenter les exclusions. Pourquoi tel service ou tel produit est-il exclu de la portée du PCA?

4 Établir les bénéfices du PCA

Un PCA génère-t-il des bénéfices financiers et non financiers?

- **Exemple de gains financiers:** réduction des coûts de mise en œuvre lors d'une remise en service à la suite d'une crise.
- **Exemple de gains non financiers:** personnel qui sait quoi faire en cas de crise réelle.

5 Établir un échéancier

Quelle sera la durée de mise en place du PCA? Quels sont les livrables à réaliser?

- **Exemple de livrables:** une politique de continuité, une analyse d'impact (plus connu sous l'appellation BIA – bilan d'impact sur les activités), une stratégie de continuité, etc. Pour avoir une liste exhaustive des livrables à réaliser, vous référer aux normes ISO 22 301 et 22 313.

6 Déterminer l'équipe du projet

Qui composera l'équipe du projet? Est-ce que l'on aura des ressources consacrées au projet?

- **Exemple de composition de l'équipe:** représentants des TI, des communications, des finances, responsables des procédures liées aux métiers, etc.

7 Déterminer la matrice RACI

Qui sera responsable de la production du ou des livrables? Qui contribuera à la réalisation des livrables? Etc. La matrice RACI[1] permettra de préciser les fonctions, les rôles et les responsabilités de chacun dans l'élaboration des livrables et des activités à réaliser.

- **Exemple de responsabilité:** les communications seront responsables d'élaborer un plan de communication de crise.

[1] responsible, accountable, consulted et informed

8 Établir un budget

Le responsable du plan de continuité (RPCA) s'appuiera sur les bonnes pratiques en gestion de projet pour estimer les coûts de la mise en place d'un PCA ainsi que les coûts récurrents. Le budget est un facteur important, qui pèsera dans la prise de décision concernant le projet.

- **Exemple de coût récurrent:** maintenance du logiciel PCA.

9 Définir les outils du projet

Quels sont les outils de gestion de projet à mettre en place? Existe-t-il déjà un cadre de référence en gestion de projet dans l'entreprise? Pour gérer, surveiller et maîtriser le projet, le RPCA s'appuiera sur les pratiques exemplaires de l'industrie.

- **Exemples d'outils de gestion:** modèles de revue de projet, modèles de suivi des livraisons et des biens livrables, etc.

10 Déterminer les contraintes

Quelles sont les contraintes qui empêcheraient le bon déroulement du projet? Quelles seraient les stratégies à définir pour les surmonter? Les contraintes peuvent différer d'une entreprise à l'autre. Cependant, deux d'entre elles tendent à revenir:

1) Le manque de leadership de la direction pourrait nuire à la réussite du projet. Le succès d'un projet PCA dépend du niveau d'implication et d'engagement de la direction. Si jamais le RPCA n'obtenait pas l'appui de sa direction, la date de livraison du projet ne serait pas respectée.

- **Exemples de stratégies pour surmonter cette contrainte:** nommer un membre de la direction comme « parrain » du projet, inclure les membres de la direction dans le comité de suivi du PCA, etc.

2) La non-disponibilité des ressources humaines pourrait ralentir le déroulement du projet. Si jamais une ressource s'absentait pour une longue période, l'activité dont elle s'occupe pourrait être retardée, ce qui risquerait d'affecter la date de livraison du projet.

- **Exemples de stratégies pour surmonter cette contrainte:** établir un calendrier des disponibilités des ressources, identifier des responsables pour chaque groupe de ressources, qui pourront au besoin fournir des remplaçants au RPCA, etc.

11 Communiquer et sensibiliser

Ce point est particulièrement important, car lorsque vous mettez en place un PCA, il est important de communiquer et sensibiliser l'ensemble du personnel dès le démarrage du projet, ainsi qu'à toutes ses étapes.

- Vous rencontrerez les directeurs, chefs de service, etc. pour leur expliquer l'importance du projet et aussi pour les informer que pendant les phases du projet et de la récurrence, certaines ressources réaliseront des livrables et d'autres auront un rôle à jouer dans le déroulement d'une crise.
- Il est important de préciser que la communication et la sensibilisation ne s'arrêtent pas une fois que le projet passe en réalisation. Bien au contraire, il faut continuer de communiquer et de sensibiliser son personnel afin de toujours avoir un PCA opérationnel.

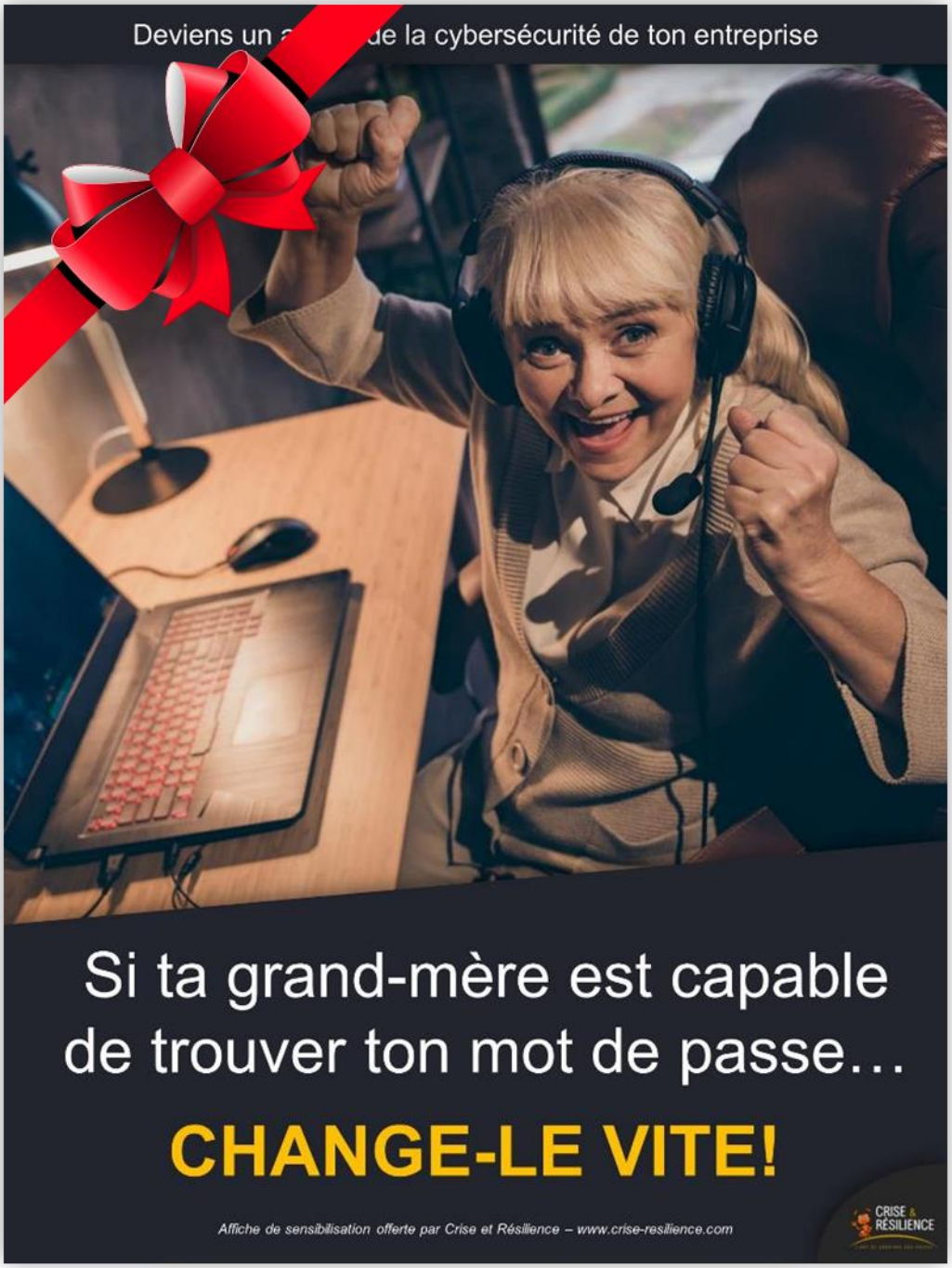
En conclusion, la continuité des activités est un sujet particulièrement vaste et un domaine en perpétuel mouvement. Pour être un outil de gestion de crise efficace, le plan de continuité des activités (PCA) doit coller aux réalités et aux besoins de chaque entreprise, et pouvoir s'adapter à l'évolution de son écosystème.

Dans cet article, seul le plan de continuité destiné à l'ensemble des activités d'une entreprise a été abordé.

Karine Maréchal Richard

SENSIBILISATION DU MOIS 👉 15 affiches à télécharger gratuitement.

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 les 15 affiches en cliquant ici

Vous souhaitez proposer une sensibilisation? Contactez-nous: info@crise-resilience.com.

BLACKOUT INFORMATIQUE

Qu'arriverait-il si votre entreprise n'avait plus accès à son système informatique pendant plusieurs heures, voire plusieurs jours?

Cet événement, connu sous le nom de « *blackout* informatique », peut avoir de graves conséquences sur vos activités professionnelles et votre vie personnelle.

Dans cet article, nous allons découvrir les causes possibles de ces incidents et les moyens de les prévenir et de les gérer efficacement.

Par Alexandre Fournier

Expert en gestion et simulation de crise

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

L'expression « ***blackout* informatique** » désigne une panne générale du système informatique d'une entreprise ou d'un individu. Un tel incident peut avoir de graves conséquences pour les entreprises et entraîner une perte de productivité, de revenus et de confiance de la part des clients.

Les individus dont le système informatique tombe en panne peuvent perdre des données personnelles importantes et avoir de la difficulté à accéder à leurs services en ligne.

« La technologie est un outil formidable, mais elle peut aussi être très fragile. Un simple *blackout* informatique peut perturber gravement les activités d'une entreprise. »

Bill Gates

Causes possibles d'un *blackout* informatique

Il est difficile d'énumérer toutes les causes possibles d'un *blackout* informatique, car de nombreux facteurs entrent en jeu, tels que la qualité et l'âge des équipements, les pratiques de maintenance et de sécurité mises en place, et les menaces auxquelles sont exposés les systèmes informatiques.

Voici néanmoins une liste non exhaustive de 20 causes possibles des pannes informatiques en fonction de leur fréquence relative:

1. Erreurs humaines
2. Infections par des logiciels malveillants
3. Attaques de pirates informatiques
4. Problèmes de câblage
5. Problèmes de réseau
6. Pannes de l'alimentation électrique
7. Échecs de l'alimentation de secours
8. Pannes des batteries de secours
9. Problèmes de matériel
10. Problèmes de refroidissement
11. Pannes de routeurs
12. Problèmes de logiciels
13. Problèmes de maintenance
14. Problèmes de système de noms de domaine (DNS)
15. Problèmes de gestion de la bande passante
16. Problèmes de filtrage de contenu
17. Problèmes de mots de passe
18. Problèmes de certificats de sécurité
19. Problèmes de licences de logiciels
20. Problèmes de configuration du réseau

Vous avez sûrement déjà vécu une indisponibilité informatique due à au moins une de ces causes. Pour ma part, je les ai toutes subies et certaines plusieurs fois…

Il y a aussi des causes externes telles que:

- Attaques de requins ou de castors
- Sabotage interne ou externe
- Changement climatique

Faites une recherche avec les mots castor et panne Internet…

Les causes possibles d'un *blackout* informatique peuvent être regroupées en quatre catégories.

Les **erreurs humaines** sont souvent à l'origine de ces incidents, qui peuvent être causés, par exemple, par une mauvaise configuration des équipements ou une utilisation inappropriée de ces derniers. La raréfaction des ressources qualifiées, résultat de la progression rapide des technologies, entraîne une pression sur une poignée de spécialistes, qui sont plus susceptibles de commettre des erreurs.

Les **problèmes matériels** sont également une cause fréquente de pannes informatiques. En effet, il n'est pas rare qu'un blackout soit causé, par exemple, par la défaillance de certains équipements ou un problème de surchauffe. L'obsolescence matérielle par manque de budget ou de temps génère aussi une fragilité des systèmes informatiques.

Les **menaces externes** comme les attaques de pirates informatiques ou les perturbations affectant les réseaux de communication peuvent également entraîner des pannes générales. On peut aussi parler de plus en plus de cyberguerre dont le but principal est de déstabiliser un pays.

Les **problèmes de logiciels** tels que les bogues ou les virus comptent également parmi les causes possibles de *blackout* informatique.

Quels seraient les impacts d'un *blackout* pour votre entreprise?

Ces *blackouts* informatiques peuvent avoir de graves conséquences pour l'entreprise et ses clients, en particulier lorsque les activités de l'entreprise dépendent fortement de ses systèmes informatiques.

Les impacts peuvent être variés et dépendent de la nature de la panne et de l'importance des systèmes informatiques pour l'entreprise. Par exemple, un *blackout* informatique peut entraîner des perturbations dans les opérations de l'entreprise, des retards dans la livraison de produits ou de services, des pertes financières, des dommages à la réputation de l'entreprise, etc.

Il pourrait également y avoir des répercussions sur les clients de l'entreprise, qui pourraient être affectés par des perturbations dans les services qu'ils reçoivent. Voici quelques impacts que vous pourriez subir dans une telle situation:

Perte de productivité: vos employés ne pourront pas travailler, ce qui risque d'entraîner une perte de productivité.

Dépassement des délais de livraison: l'impossibilité d'accéder à vos données ou à vos systèmes de gestion de commandes fera augmenter les délais de livraison.

Problèmes de collaboration: vos employés ne pourront plus accéder aux outils collaboratifs.

Perte de données: vous perdrez votre historique et vos documents essentiels.

Mauvaise gestion de la relation client: il sera difficile de répondre aux demandes de vos clients de manière efficace.

Impact sur la réputation: votre réputation pourrait être fortement affectée.

Perte de revenus: vous ne pourrez pas honorer vos commandes, clore vos contrats, etc.

Coûts de remise en état: vous allez dépenser de l'argent pour réparer vos systèmes informatiques et remettre en état vos données perdues.

Défaillance de l'approvisionnement: vous ne pourrez pas accéder à vos systèmes de gestion de l'approvisionnement et pourriez manquer de matières premières ou de composants nécessaires à votre production.

Problèmes juridiques: vous ne pourrez pas respecter vos obligations contractuelles, ce qui pourrait entraîner des problèmes d'ordre juridique.

Problèmes de trésorerie: vous perdez des revenus, ce qui se soldera en problèmes de trésorerie.

Problèmes de conformité: vous ne pourrez pas vous conformer aux réglementations, ce qui pourrait entraîner des problèmes de conformité.

Perturbation de la chaîne d'approvisionnement: vous ne pourrez plus suivre vos commandes et vos expéditions, ce qui perturbera la chaîne d'approvisionnement et minera les relations avec vos fournisseurs et vos clients.

Problèmes de sécurité: vous serez plus vulnérable aux cyberattaques.

Problèmes de gestion des ressources humaines: vous ne pourrez plus gérer les salaires, les congés, etc.

Problèmes de gestion de la chaîne logistique: vous ne pourrez plus gérer la chaîne logistique de manière efficace.

Impact sur les partenariats et fournisseurs: votre relation avec vos partenariats et fournisseurs serait perturbée.

> **« La crise est un appel à l'innovation, à la créativité et à la solution. »**
>
> *Steve Jobs*

Comment réduire l'impact?

Il est important pour les entreprises de mettre en place des mesures de prévention et de gestion des *blackouts* informatiques afin de minimiser leurs impacts sur les activités et les clients de l'entreprise.

Ces mesures peuvent inclure la mise en place de plans de continuité des activités, la redondance des systèmes informatiques, la formation du personnel aux bonnes pratiques de gestion des incidents, etc.

Voici 27 pistes de solutions qui pourraient vous aider en cas de panne informatique. Cela dit, il est important de vous préparer AVANT qu'un incident ne survienne – cela augmentera vos chances de survie.

Perte de productivité

- Mettre en place des solutions de travail à distance pour permettre aux employés de travailler à partir de leur domicile.
- Utiliser des outils de collaboration en ligne pour permettre aux employés de travailler ensemble de manière efficace même s'ils ne sont pas physiquement présents au bureau.
- Former les employés à l'utilisation de ces outils de collaboration en ligne pour qu'ils puissent travailler de manière efficace même en cas de perturbation.

Perte de données

- Mettre en place des sauvegardes régulières pour s'assurer que les données importantes sont sauvegardées et peuvent être restaurées en cas de perte de données.
- Utiliser des outils de synchronisation des données pour s'assurer que les données sont accessibles depuis plusieurs appareils et que les employés peuvent y accéder même en cas de perturbation.
- Former les employés à l'utilisation de ces outils de synchronisation pour qu'ils puissent continuer à travailler en cas de perturbation.

Perte de revenus

- Mettre en place des processus de secours pour continuer à traiter les commandes et à générer des revenus en cas de perturbation informatique.
- Travailler avec des fournisseurs de secours pour s'assurer de toujours avoir accès à des matières premières et des composants en cas de défaillance de l'approvisionnement.
- Offrir des remises ou des avantages aux clients pour compenser les perturbations causées par le *blackout* informatique.

Problèmes de trésorerie

- Mettre en place des processus de secours pour continuer à générer des revenus en cas de perturbation informatique.
- Travailler avec des fournisseurs de secours pour s'assurer de toujours avoir accès à des matières premières et des composants en cas de défaillance de l'approvisionnement.
- Prévoir des réserves de trésorerie pour faire face aux perturbations et aux pertes de revenus temporaires.

Problèmes de sécurité

- Mettre en place des sauvegardes régulières pour s'assurer que les données importantes sont sauvegardées et peuvent être restaurées en cas de cyberattaque.
- Utiliser des outils de sécurité de secours pour protéger les systèmes informatiques en cas de perturbation.
- Former les employés aux bonnes pratiques de sécurité informatique pour réduire les risques de cyberattaque.

Défaillance dans l'approvisionnement

- Mettre en place des processus de secours pour continuer à traiter les commandes en cas de perturbation informatique.
- Travailler avec des fournisseurs de secours pour s'assurer de toujours avoir accès à des matières premières et des composants en cas de défaillance de l'approvisionnement.
- Prévoir des stocks de sécurité pour s'assurer qu'il y a suffisamment de matières premières et de composants pour continuer à produire en cas de perturbation.

Problèmes dans la chaîne logistique

- Mettre en place des outils de gestion de la chaîne logistique de secours pour permettre aux employés d'accéder au suivi d'inventaire même en cas de panne informatique.
- Utiliser des outils de synchronisation des données pour s'assurer que les données logistiques sont accessibles depuis plusieurs appareils et que les employés peuvent y accéder même en cas de perturbation.
- Former les employés à l'utilisation de ces outils de gestion de la chaîne logistique de secours.

Coûts de remise en état

- Mettre en place des contrats de maintenance et de soutien pour s'assurer que les systèmes informatiques sont entretenus et peuvent être réparés rapidement en cas de perturbation.
- Utiliser des outils de gestion de la qualité pour s'assurer que les systèmes informatiques sont fiables et éviter les perturbations.
- Former les employés aux bonnes pratiques de gestion de l'informatique pour réduire les risques de perturbation.

Fragilisation des relations d'affaires

- Mettre en place des processus de secours pour respecter les obligations contractuelles en cas de perturbation informatique.
- Travailler avec des avocats pour évaluer les risques et les obligations en cas de perturbation.
- Négocier avec les parties contractantes pour trouver des solutions de rechange en cas de perturbation.
- Communiquer avec les fournisseurs et les partenaires pour les informer de la situation et de la manière dont l'entreprise compte redresser la situation.

Bonnes pratiques pour prévenir les *blackouts* informatiques

Il est possible de mettre en place certaines mesures pour prévenir les *blackouts* et protéger les systèmes informatiques des entreprises et des individus.

Tout d'abord, il est recommandé de mettre en place des dispositifs de sécurité pour protéger les systèmes contre les menaces externes telles que les attaques informatiques ou les perturbations des réseaux de communication. Ces dispositifs peuvent inclure des pare-feu (*firewalls*) et des antivirus. Il est également important de former les utilisateurs aux bonnes pratiques informatiques afin de minimiser les risques d'erreurs humaines, qui sont souvent à l'origine des pannes.

La maintenance régulière des équipements et des logiciels est également un élément clé de la prévention de ces incidents. Cela peut inclure la mise à jour des logiciels, la vérification de la bonne utilisation des équipements et la réparation des défauts matériels.

Enfin, il est essentiel de mettre en place des dispositifs de sauvegarde des données pour protéger les informations importantes des entreprises et des individus. Cela peut se faire par le biais de sauvegardes externes ou de services de stockage de données dans le nuage (*cloud*).

En somme, la prévention des *blackouts* informatiques passe par une bonne protection des systèmes informatiques contre les menaces externes, une formation adéquate des utilisateurs, une maintenance régulière des équipements et des logiciels, de même que par la mise en place de dispositifs de sauvegarde des données.

Évaluer votre résilience en cliquant ici

Comment se préparer à un *blackout* informatique?

La gestion d'un *blackout* informatique est un défi important pour les entreprises, qui dépendent de plus en plus de leurs systèmes informatiques. Un tel incident, qui perturbe ou interrompt complètement les services informatiques d'une entreprise pour une durée indéterminée, peut avoir de graves conséquences pour l'entreprise, surtout si ses activités dépendent fortement de ses systèmes informatiques.

Pour gérer efficacement un *blackout*, il est important de disposer d'un plan de continuité des activités (PCA), qui définit les actions à entreprendre en cas d'incident informatique. Un PCA doit prévoir des mesures de secours pour assurer la continuité des activités de l'entreprise et minimiser les impacts de l'incident sur les clients et sur l'entreprise elle-même.

Le PCA doit inclure une liste des tâches à accomplir et un plan de communication pour informer les parties prenantes de l'état de l'incident et de la façon dont il est géré. Il doit également prévoir des mesures de protection des données et des mesures de reprise après sinistre pour assurer la continuité de l'activité de l'entreprise.

Il est également important de s'assurer que le personnel de l'entreprise est formé à la gestion des incidents informatiques et qu'il est en mesure de mettre en œuvre les mesures prévues dans le PCA. La formation du personnel et la réalisation d'exercices réguliers pour mettre en pratique le plan de continuité peuvent aider l'entreprise à être mieux préparée en cas de *blackout* informatique.

Enfin, il est essentiel de mettre en place des mesures de redondance des systèmes informatiques pour minimiser le risque de *blackout* informatique. La redondance des systèmes informatiques consiste à disposer de plusieurs copies des données et des applications critiques afin de pouvoir continuer à fonctionner en cas de défaillance d'un système. Cela peut se faire en utilisant des serveurs de secours, en stockant des copies de données dans le nuage (*cloud*), en utilisant des dispositifs de stockage en réseau (SAN), etc.

Il est également important de mettre en place des mesures de sécurité pour protéger les systèmes informatiques contre les menaces externes telles que les virus, les pirates informatiques, etc. Ces mesures peuvent inclure la mise en place de pare-feu, de logiciels de protection contre les virus, de systèmes de détection des intrusions, etc.

En somme, la gestion d'un *blackout* informatique requiert une planification et une préparation rigoureuses, de même que la mise en place de mesures de prévention et de redondance pour minimiser le risque de défaillance des systèmes informatiques. En s'assurant de disposer d'un PCA solide et d'un personnel bien formé, les entreprises seront mieux préparées pour faire face à ces événements et limiter les impacts sur leur activité et leurs clients.

Comment agir lors d'un *blackout* informatique?

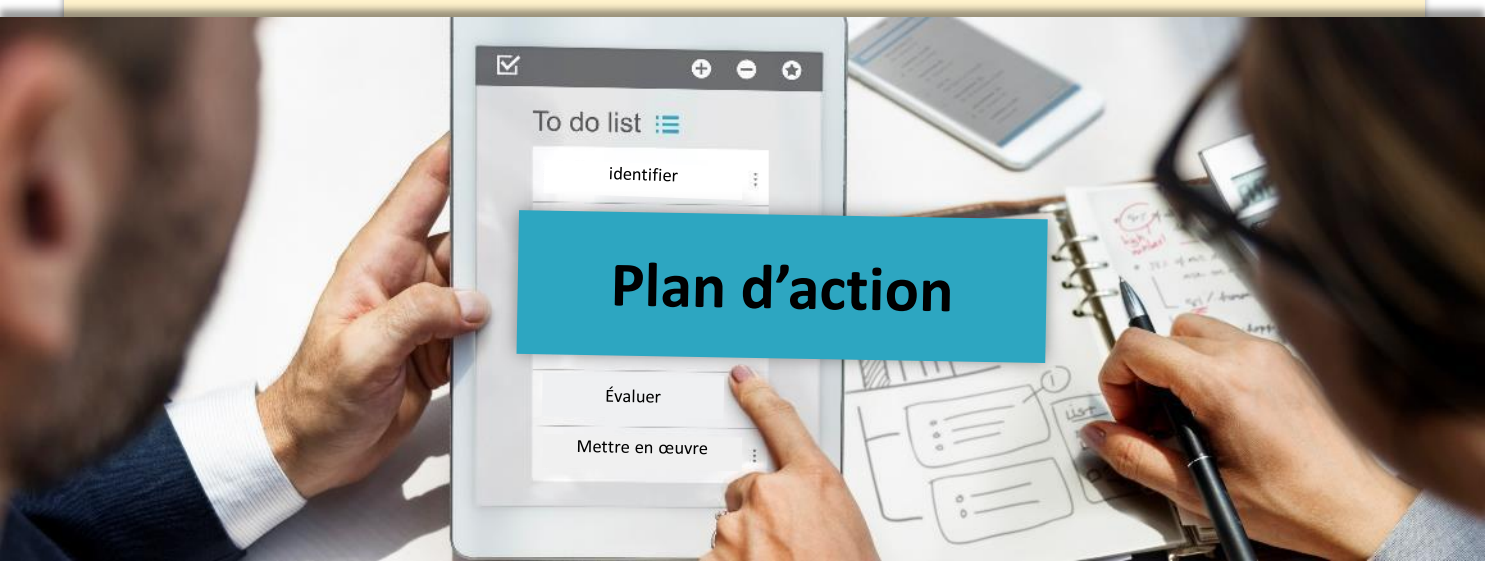
La gestion d'un *blackout* informatique consiste principalement à assurer la continuité des activités de l'entreprise et à minimiser les impacts de l'incident sur les clients et sur l'entreprise elle-même. Pour cela, on s'appuie sur un plan de continuité des affaires (PCA) et on applique un plan de gestion de crise en lien avec l'événement perturbateur.

On vous propose ci-dessous un **plan d'action générique et non exhaustif**:

- **Identifier et localiser l'incident.** La première étape consiste à identifier l'origine de l'incident et à localiser les équipements et les services affectés. Cela peut se faire en utilisant les outils de surveillance et de diagnostic des systèmes informatiques, en consultant les journaux d'événements, en interrogeant le personnel, etc.
- **Évaluer l'impact de l'incident.** Une fois l'incident identifié et localisé, il est important de l'évaluer afin de déterminer l'ampleur des dégâts et les impacts sur l'entreprise et ses clients. Cela peut se faire en analysant les données de performance et de disponibilité des systèmes informatiques, en interrogeant le personnel sur les perturbations observées, etc.
- **Mettre en œuvre les mesures de secours.** En fonction de l'impact de l'incident, il peut être nécessaire de mettre en œuvre des mesures de secours pour assurer la continuité des activités de l'entreprise et minimiser les répercussions sur les clients. Ces mesures peuvent inclure l'application d'un plan de continuité des affaires (PCA), d'un plan de reprise informatique, la mise en place ou la reconstruction de serveurs de secours, le transfert de données vers le nuage (cloud), l'utilisation de dispositifs de stockage en réseau (SAN), la restauration de données, etc.
- **Communiquer avec les parties prenantes.** Il est important de communiquer régulièrement avec les parties prenantes (clients, employés, fournisseurs, etc.) afin de les informer de l'état de l'incident et de la façon dont il est géré. Cela peut se faire en utilisant différents canaux de communication (intranet, réseaux sociaux, messagerie électronique, etc.), en s'assurant de fournir des informations précises et à jour.
- **Analyser les causes de l'incident.** Une fois l'incident résolu, il faut l'analyser. Cela peut se faire lors de retour d'expérience en effectuant des entretiens avec le personnel, en utilisant des outils d'analyse de logs, en consultant les journaux d'événements, etc.
- **Mettre en œuvre les mesures de prévention.** Une fois les causes de l'incident identifiées, il convient de mettre en place des mesures de prévention pour éviter de futurs *blackouts* informatiques. Ces mesures peuvent inclure la mise à jour des logiciels et des équipements, la formation du personnel aux bonnes pratiques de gestion des incidents, la mise en place de plans de continuité des activités (PCA), etc.
- **Préparer la reprise après sinistre.** En cas de panne informatique grave, il peut être nécessaire de prévoir une reprise après sinistre pour assurer la continuité de l'activité de l'entreprise. Cela peut inclure la mise en place de plans de reprise de l'activité, la création de copies de secours des données et des logiciels, l'instauration de processus de vérification et de test des systèmes informatiques, etc.

Il est important de noter que le plan d'action détaillé ci-dessus est un exemple générique et qu'il peut être adapté en fonction des besoins et des réalités de l'entreprise. Il est recommandé de mettre en place un plan de continuité des activités (PCA) qui précise les actions à entreprendre en cas de *blackout* informatique et qui prend en compte les spécificités de l'entreprise.

De plus, il faut s'assurer que le personnel de l'entreprise est formé à la gestion des incidents informatiques et qu'il est en mesure de mettre en œuvre les mesures prévues dans le PCA. La formation du personnel et la réalisation d'exercices réguliers pour mettre en pratique le plan de continuité peuvent aider l'entreprise à être mieux préparée en cas de *blackout* informatique.



Quelles sont les chances de survie d'une entreprise victime d'un *blackout* informatique?

Il est difficile de donner une réponse précise quant aux chances de survie d'une entreprise qui subit un *blackout* informatique, car cela dépend de nombreux facteurs tels que la nature et l'étendue de l'incident, la durée de l'interruption des activités, la réputation de l'entreprise auprès de ses clients, la qualité de ses mesures de prévention et de protection, et son niveau de dépendance aux technologies de l'information.

En général, plus l'incident est grave et plus la durée de l'interruption des activités est longue, plus les chances de survie de l'entreprise sont faibles. De même, si l'entreprise a une mauvaise réputation auprès de ses clients ou si elle est dépendante des technologies de l'information, elle sera plus vulnérable face à un *blackout* informatique.

Une panne informatique représente une source de stress importante pour une entreprise et peut même entraîner sa faillite.

Selon une étude de Kaspersky, les coûts moyens liés à un *blackout* informatique sont de 656 000 € ou 946 000 $ CA par entreprise en France.

En conclusion

Les *blackouts* informatiques sont des événements volontaires ou involontaires qui affectent les systèmes informatiques d'une entreprise ou d'une organisation. Ces incidents peuvent avoir de graves conséquences pour les entreprises et entraîner une perte de productivité, des coûts supplémentaires et des dommages à la réputation. Il est donc nécessaire pour les entreprises de prendre des mesures préventives et de disposer de plans de secours adéquats.

Parmi les mesures préventives, il est très fortement recommandé de mettre en place une solution de sauvegarde sécuritaire et à l'épreuve des cyberattaques, de même qu'un système de surveillance de vos équipements pour détecter les problèmes potentiels avant qu'ils ne se produisent. Il est également important de s'assurer que les systèmes informatiques sont protégés contre les virus et les logiciels malveillants, qui peuvent entraîner des pannes.

Afin de pouvoir répondre aux impacts d'un *blackout* informatique, il est essentiel d'avoir un plan de continuité des affaires (PCA) en place et à jour qui vous permettra de reprendre rapidement vos activités. Ce PCA devra intégrer un plan de gestion de crise, des procédures de continuité des activités sans recours à l'informatique, un plan de reprise informatique agile et adaptable en fonction de la crise et enfin un plan de communication de crise.

Vous l'aurez compris, afin de minimiser les impacts dus à l'indisponibilité de vos outils informatiques, il est donc essentiel… que dis-je… il est VITAL si vous souhaitez survivre de vous préparer avant que vous ne subissiez un *blackout* informatique. Si vous tenez à votre entreprise, alors faites le nécessaire rapidement pour mettre en place un plan de continuité des affaires et un plan de gestion de cybercrise.

Alexandre Fournier

Pour les sceptiques, voici une liste non exhaustive d'articles de presse au sujet d'entreprises qui ont subi des *blackouts* informatiques en 2022

Les Échos, 5 décembre 2022

L'hôpital de Versailles victime d'une **cyberattaque**

TVA Nouvelles, 6 novembre 2022

Retards et annulation: la **panne informatique** corrigée chez WestJet

Le Journal de Montréal, 25 octobre 2022

La messagerie WhatsApp rétablie après une **panne informatique mondiale**

lebigdata.fr, 20 octobre 2022

Data Center: comment un simple **incendie** a ravagé le Web coréen?

20 minutes, 28 septembre 2022

Brest: Le centre hospitalier paralysé par une **panne informatique**

les affaires, 15 septembre 2022

Reprise graduelle des activités de loterie chez Loto-Québec à la suite d'une **panne informatique**

lebigdata.fr, 19 août 2022

Incendie dans un datacenter Google, 3 blessés: comment éviter ces drames?

Slate, 7 août 2022

La **canicule fait crasher le système informatique** des hôpitaux londoniens

AFP, 15 juin 2022

Suisse: fermé après une **panne informatique**, l'espace aérien rouvre

Les Échos, 31 mai 2022

Brest: Le centre hospitalier paralysé par une **panne informatique**

Le Journal de Montréal, 28 février 2022

Toyota suspend sa production au Japon après une probable **cyberattaque**

D'après le sondage 2022 sur la résilience des centres de données d'Uptime, 80 % des gestionnaires et opérateurs de centres de données ont subi une panne au cours des trois dernières années.
Source: silicon.fr

Soyez prêt à affronter toute crise qui pourrait menacer votre entreprise

PROFITEZ
500 $
de réduction
jusqu'au 15 février 2023

Inscrivez-vous dès maintenant à nos formations pour protéger votre entreprise contre les menaces.

www.crise-resilience.com

Oyez, oyez, braves lecteurs!

Envie de devenir un pro de la gestion de crise cyber, c'est le moment ou jamais !

Grâce à notre jeu-concours d'avril, organisé par Crise & Résilience, remportez une de nos formations !

C'est l'occasion parfaite pour célébrer la sortie de notre magazine.

Plus vous utiliserez le hashtag **#MagazineCriseEtRésilience** plus vous aurez de chances de gagner!

Participez dès maintenant et peut-être que vous serez l'un des 2 prochains gagnants!

1, 2, 3… partagez!

Avertissement : Ce jeu est en cours d'approbation. Sa sortie dépend de l'accord des autorités compétentes.
Si nous ne recevons pas les autorisations requises, nous serons contraints de ne pas le lancer en avril.

PRÉVENIR VAUT MIEUX QUE GUÉRIR…

Faites un bilan de l'état de santé de la sécurité de votre entreprise, sinon…

Il y a quelques jours, je consultais mon dentiste pour la sixième fois en un an. Ça fait beaucoup, me direz-vous! Croyez-moi, je le pense aussi, mais je n'aurais pas été aussi fidèle aux rendez-vous si je n'avais pas perdu trois dents auparavant.

Par Cyrille Augustin Molemb Beal

Conseiller en sécurité de l'information

Titulaire d'un master en TI, il possède une douzaine d'années d'expérience dans les TI, incluant une dizaine dans la cybersécurité.

En effet, je ressentais régulièrement des douleurs dentaires sans que cela m'empêche de continuer à mâcher des aliments, jusqu'à ce fameux soir où ma cavité dentaire a enflé tel un ballon et mes mâchoires inférieures et supérieures ne pouvaient plus se toucher sans que je ressente une atroce douleur. La suite, nous la connaissons déjà: trois dents perdues et quelques milliers de dollars dépensés. Quel gâchis!

Si j'avais consulté mon médecin plus tôt, non seulement je n'aurais pas dépensé un tel montant d'argent, mais surtout, j'aurais encore toute ma dentition aujourd'hui.

Cette histoire illustre parfaitement la réalité de plusieurs entreprises canadiennes en lien avec la cybercriminalité: elles se laissent « tuer à petit feu » et s'inscrivent davantage dans la réaction après incident que dans la prévention.

Et le mal, quant à lui, ne cesse de se répandre…

Selon sondage[1] de CIRA sur la cybersécurité de 2022, trois entreprises canadiennes sur dix (29 %) ont subi une violation des données de leurs clients et/ou de leurs employés. « Avant la pandémie, seuls 18 % disaient en avoir fait l'expérience. »

Le sondage précise également qu'en 2022 :

29% des entreprises ont subi une violation de données d'informations de clients ou d'employés, ce qui est une augmentation par rapport à 18% avant la pandémie.

15% des organisations ont signalé avoir perdu des clients en raison d'une attaque, ce qui est le double du niveau pré-pandémique.

25% d'organisations canadiennes de plus ont souscrit une assurance cybersécurité en 2022 malgré les coûts et les exigences croissants.

55% considèrent leur organisation comme plus vulnérable aux cybermenaces car leurs employés travaillent à distance.

63% des organisations considèrent la souveraineté des données comme plus importante que le prix lors de la sélection d'un fournisseur de services de cybersécurité.

96% des organisations ont une formation obligatoire de sensibilisation à la cybersécurité pour certains employés, contre 87% avant la pandémie.

82% des professionnels de la sécurité indiquent que leur organisation dispose d'un plan de réponse aux cyberincidents, tandis que 6 organismes sur 10 ont utilisé ce plan dans les 12 derniers mois.

55% des professionnels de la cybersécurité sont au courant du projet de loi C-27 et 59% d'entre eux sont inquiets de son impact potentiel sur leur organisation. Le secteur privé semble moins préparé à mettre en place de nouvelles exigences.

Au moins **25 000 $** ont été versés par les organisations qui ont payé une rançon.

29%

des entreprises ont subi une violation de données d'informations de leurs clients ou employés

Vous avez certainement compris au travers des statistiques ci-dessus que vous devez faire plus pour vous protéger et protéger votre entreprise du cybercrime – les dommages en cas d'incident ou d'attaque pourraient vous coûter très cher.

[1] Source de ce sondage : https://www.cira.ca/fr/ressources/cybersecurite/rapport/sondage-cybersecurite-2022.

Vous êtes aussi capable de voir à quel point vous seriez paralysé si votre site Web tombait en panne pendant 24 heures, ou encore si vous étiez incapable de récupérer vos documents stratégiques à quelques heures d'une rencontre avec le client le plus important de votre vie, ou bien avec l'investisseur que vous attendiez depuis longtemps.

Cependant, qu'il me soit permis de vous dire qu'au-delà de ce que vous perdrez potentiellement à la suite d'un cybercrime, il y a ce que vous gagnerez assurément en réalisant un diagnostic de votre santé cybernétique.

Qu'est-ce que vous gagnerez à faire un bilan?

Une entreprise est essentiellement constituée d'actifs humains, matériels et immatériels, qui, mis ensemble, produisent des biens et services pour des clients, le tout avec un objectif de rentabilité. Assurer la pérennité d'une entreprise, c'est donc assurer la pérennité de ses actifs.

Cependant, comme le corps humain peut subir des attaques de toutes sortes (infections bactériennes ou virales, accidents, vieillissement, etc.), les actifs d'une entreprise peuvent faire l'objet d'attaques qui pourraient mettre à mal le fonctionnement et même l'existence de l'entreprise. Au premier rang de celles-ci se trouve le cybercrime, ou cybercriminalité.

L'être humain a tout à gagner, pour vivre longtemps et en bonne santé, à réaliser régulièrement un contrôle de santé chez un médecin et à soigner les problèmes de santé détectés avant qu'il ne soit trop tard.

Selon votre profil de risque (antécédents familiaux, exposition aux menaces du fait de votre activité professionnelle, etc.), vous serez amené à rencontrer votre médecin plus ou moins souvent que les autres.

De la même façon, toute entreprise sérieuse doit de se garder en forme le plus longtemps possible et identifier les situations à risque aussitôt que possible pour intervenir lorsqu'il est encore temps. Si, par exemple, vous attendez d'être attaqué pour vous rendre compte que vous aviez des vulnérabilités dans votre site Web, votre logiciel de paie ou la base de données de tous vos clients, il sera trop tard et des dommages tangibles et intangibles pourraient détruire votre entreprise.

C'est pourquoi il faut faire un bilan de l'état de santé de la sécurité de votre entreprise à une fréquence régulière, au début et à la fin d'un projet d'envergure, lors de l'intégration de nouveaux systèmes ou en cas de changement majeur. Ce bilan doit bien entendu être réalisé par des professionnels de la cybersécurité, reconnus et éprouvés.

Ces bilans réguliers vous permettront entre autres de:

- cartographier votre système d'information (si ce n'est déjà fait);
- identifier vos postures de sécurité et comparer vos pratiques de sécurité avec les normes de l'industrie pour vous assurer d'avoir le niveau requis de protection;
- gérer vos processus d'affaires en toute sécurité et garantir un environnement de travail sain;
- acquérir une bonne réputation et la préserver;
- gagner la confiance de vos partenaires et clients;
- augmenter votre productivité et votre rentabilité;
- mieux faire votre analyse de besoins en matière de solutions de sécurité et mieux gérer vos dépenses;
- obtenir des recommandations concrètes et faciles à mettre en place.

Cyberswat vous propose une liste des actifs et services dignes d'intérêt lors d'un bilan régulier de cybersanté:

- Vos principaux logiciels et principales plateformes d'affaires;
- Votre site Web;
- Votre parc informatique;
- Les sauvegardes de vos données;
- Votre système de messagerie;
- La gestion de vos ressources humaines et des accès;
- Votre mécanisme de gestion du télétravail;
- La gestion de vos dispositifs mobiles;
- La gestion des codes utilisateurs et des mots de passe;
- Vos réseaux sans fil;
- L'utilisation de l'Internet des objets (IoT);
- La gestion des réseaux sociaux;
- La gestion de l'infonuagique (*cloud*).

Quels sont les principaux actifs à évaluer?

Si une entreprise (TPE, PME ou multinationale) dispose de plusieurs actifs informationnels ou systèmes d'information, il n'en demeure pas moins que tous ne jouent pas le même rôle et ne revêtent pas la même importance.

Un des éléments clés du bilan de cybersanté consiste à identifier le ou les systèmes informatiques les plus importants de l'entreprise et à se concentrer sur ceux-ci. Il faut également identifier les situations mettant l'entreprise à risque d'être la cible d'une cyberattaque. C'est un peu comme si vous étiez chez le docteur et que vous deviez parler de vos antécédents familiaux!

Il est primordial que tous les actifs d'une entreprise soient classifiés selon leur niveau de criticité afin de prioriser les actions de diagnostic et de maintenance.

Toutefois, il convient de préciser que l'homme reste le principal actif pour toute entreprise, en plus d'être le maillon faible de la chaîne sécuritaire. Il est donc important de réaliser des tests de contrôle des employés afin de mieux faire face aux menaces de type ingénierie sociale et hameçonnage, tout en formant et en sensibilisant les employés aux enjeux de cybersécurité actuels.

Comment se passe la réalisation d'un bilan de santé en cybersécurité?

Plusieurs normes internationales en matière d'audit de sécurité des systèmes d'information peuvent servir de cadre de référence pour la réalisation d'un diagnostic de sécurité.

Au Groupe Cyberswat, notre expertise avérée dans le domaine de la cybersécurité nous a permis de faire une sélection parcimonieuse des éléments clés à mettre en place, éléments qui sont particulièrement critiques dans le contexte des PME. Inspiré de la norme internationale ISO/IEC 27002:2013 et du référentiel de cybersécurité de l'organisme américain NIST, notre diagnostic permet d'obtenir des recommandations et des pistes de solutions afin de diminuer la probabilité et l'impact d'une atteinte dans un environnement informatique.

« L'évaluation est la clé de la réussite. Si vous ne savez pas où vous en êtes, vous ne savez pas où vous allez. »
Benjamin Franklin

Les principales étapes d'un processus de diagnostic de sécurité seront:

1 La préparation de la mission de diagnostic

La phase préparatoire consiste à prendre toutes les dispositions sur le plan organisationnel et logistique pour garantir le bon déroulement de l'activité. Elle est essentiellement constituée d'une entrevue de type semi-dirigée réalisée par des experts en cybersécurité avec les principaux acteurs du système d'information de votre entreprise. Au cours de cette importante séance de travail, tous les éléments clés seront évoqués, notamment les parties du système d'information devant faire l'objet du diagnostic, la méthodologie de travail, les résultats attendus et l'élaboration du rapport. La bonne nouvelle dans tout ça, c'est que votre entreprise n'a rien de particulier à préparer pour cette rencontre, ce qui allège votre charge de travail. La présence des cadres décisionnaires de votre entreprise à l'entrevue, comme les directeurs des finances ou des TI, est un gage de succès de l'activité.

2 La réalisation du diagnostic

Le diagnostic de sécurité proprement dit est effectué en collaboration avec les personnes responsables du parc informatique et/ou du site Web de votre entreprise. À l'issue des séances de travail, l'équipe d'experts en cybersécurité passera en revue l'ensemble des informations recueillies et procédera à l'élaboration des recommandations.

3 L'élaboration du rapport

Le rapport de diagnostic sera accompagné d'un plan d'action en matière de cybersécurité, qui guidera les responsables de votre entreprise chargés de sa mise en œuvre, et de l'assignation, de la priorisation et de l'application des recommandations du diagnostic et de toute autre intervention post-diagnostic (p. ex., test d'intrusion). Une réunion de clôture permettra aux experts de présenter les conclusions du diagnostic et les recommandations formulées. Comme un rapport médical, le rapport de diagnostic présentera:

- une appréciation du niveau de santé général de l'environnement informatique analysé;
- un ensemble de recommandations, priorisées par niveau de risque (critique, élevé, modéré, faible);
- une explication des conséquences possibles si la situation n'est pas corrigée (p. ex. fuite de données, attaque de rançongiciels, perte de disponibilité du service, etc.).

4 Le suivi post-diagnostic

Selon les besoins de l'entreprise, la phase post-diagnostic peut intégrer le suivi de la mise en œuvre des recommandations formulées lors du diagnostic. Les experts en cybersécurité pourront alors, à fréquence définie, réaliser des contrôles de sécurité et évaluer le niveau d'évolution de l'entreprise.

En conclusion

Malgré l'évolution croissante du cybercrime, les expertises en matière de cybersécurité sont de plus en plus poussées et à même de répondre à l'ingéniosité malsaine des cyberdélinquants. Il revient aux entreprises, notamment aux TPE et aux PME, d'assurer la sécurité de leur patrimoine informationnel en tirant parti de cette expertise pour prévenir et contrecarrer les actions des mauvais acteurs de notre cyberespace.

Le groupe Cyberswat se place aux côtés des entreprises dans ce combat pour préserver leurs acquis grâce à ses experts et à ses services taillés sur mesure pour chaque entreprise.

Cyrille Augustin Molemb Beal

L'INFONUAGIQUE… C'EST PAS MAGIQUE!

On pourrait croire que l'infonuagique règle tous les problèmes… voici une belle croyance!

Depuis que le nuage s'est démocratisé, les entreprises prennent un virage numérique à toute vitesse, parfois sans avoir lu les petites lignes au bas du contrat. Une erreur qui peut mener l'entreprise à sa perte.

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.

De plus en plus, avec:

- l'augmentation de la quantité de données à gérer;
- les coûts de fonctionnement des infrastructures informatiques en interne;
- la rareté et l'hyper spécialisation des ressources;
- l'évolution permanente des technologies;
- et toutes les autres bonnes raisons,

les entreprises se tournent de plus en plus vers l'infonuagique.

Dans de ce virage numérique à grande, voire à très grande vitesse, la priorité, c'est la réduction des coûts. On fait fi de la réflexion sur la souveraineté des données, on néglige de penser à l'indisponibilité éventuelle du fournisseur, ou encore on dédaigne les sauvegardes. Combien de fois ai-je entendu:

« On verra ça plus tard! »

ou encore

« Bin quoi, le fournisseur s'occupe de tout… »

Adieu à toute rationalité qui permettait d'avoir une vision à long terme. Bienvenue au pays des licornes.

Loin de moi l'idée que l'infonuagique, « ce n'est pas bien ». Au contraire, je pense que c'est une superbe occasion de s'alléger d'une partie de la gestion des TI. Mais pas à n'importe quel prix!

Dans cet article, nous partagerons quelques principes de base avec vous permettant de limiter l'impact en cas d'indisponibilité de votre fournisseur infonuagique.

« J'ai tout perdu après l'incendie d'OVH. »

Lors que vous migrez la totalité de votre informatique chez un fournisseur infonuagique et que celui-ci est inaccessible (peu importe la raison), il ne vous reste, pour maintenir vos activités, que ce que vous avez en local sur vos ordinateurs de bureau.

C'est-à-dire pas grand-chose, surtout si vous avez décidé de tout externaliser chez votre fournisseur préféré.

Il se peut en effet que vous perdiez aussi votre messagerie, vos outils de réunion, possiblement votre téléphonie, vos fichiers, vos applications essentielles, vos listes de clients, fournisseurs, commandes, stocks, factures, etc.

Bref, vous êtes dans la « Me…. »!

Pour mieux comprendre l'impact, coupez la connexion réseau sur votre ordinateur et voyez ce que vous pouvez faire… pas grand-chose, j'imagine.

Vous aurez donc besoin de plans pour:

- Gérer la crise que l'indisponibilité va générer;
- Maintenir vos activités sans informatique;
- Reconstruire (éventuellement) votre informatique.

Pour gérer la crise, ça va vous prendre au minimum un moyen de communiquer (accès à un téléphone ou à une boîte de messagerie, liste de contacts avec numéros de téléphone et adresses électroniques) et des outils et procédures de gestion de crise de base.

ON CASSE LES CROYANCES!

Le fournisseur est responsable de tout. FAUX

Il est responsable de la mise à disposition et de la sécurisation de ses infrastructures. Il met en place des SLA que vous ne pouvez pas modifier.

Vous êtes seul responsable de la sécurisation, de l'intégrité et de la sauvegarde de vos données.

Le fournisseur s'adapte à nos besoins. FAUX

Il vous fournit un service clés en main et vous vous adaptez à son service.

Le nuage est plus sûr. FAUX

Il y a plusieurs exemples qui montrent hélas! le contraire: incendies, cyberattaques, indisponibilités diverses, etc.

Le nuage est redondant. VRAI-FAUX

Cela dépend du fournisseur: certains le sont et d'autres ne le sont pas.

De plus, certains fournisseurs proposent un service de redondance. Il est alors de la responsabilité du client de souscrire à ce service pour en profiter.

Il y a aussi des pannes, soit directement chez le fournisseur, soit dans la chaîne d'accès au fournisseur.

Tous les fournisseurs sont certifiés. FAUX

Malheureusement, certains fournisseurs infonuagiques ne sont pas certifiés ISO 22017, CSA STAR, SecNumCloud ou Cloud Confidence.

L'infonuagique, c'est abordable. VRAI-FAUX

Cela dépend de votre utilisation et des services auxquels vous souscrivez – le prix peut augmenter rapidement.

De plus, les fournisseurs peuvent modifier leurs tarifs à la hausse (ce qui devrait arriver avec la crise en Europe).

Je peux changer de fournisseur facilement. FAUX

Quitter un fournisseur reste complexe, surtout s'il a des applications uniques. De plus, la récupération des données peut être excessivement coûteuse.

Le nuage est sécuritaire. VRAI-FAUX

Cela dépend des services auxquels vous souscrivez et de vos connaissances en matière de gestion de ces services (ils requièrent généralement des connaissances pointues).

Une fois que vous avez ce qu'il faut pour communiquer, vous devez maintenir ou reprendre vos activités essentielles, surtout celles qui vous permettront de conserver vos clients et de préserver votre trésorerie.

Dans le cas d'un sinistre chez votre fournisseur (ex. incendie d'OVH), vous devrez activer votre plan de reprise informatique (si vous avez un contrat à cet effet).

Dans le cas d'une cyberattaque sur vos infrastructures hébergées chez votre fournisseur, il est fort possible que la solution de tolérance de panne (redondance de vos systèmes) soit elle aussi compromise.

Et dans le cas où votre fournisseur est indisponible à la suite d'une cyberattaque…

Oups!

Il va falloir attendre que le fournisseur soit lui-même à nouveau disponible, ce qui peut prendre plusieurs jours, voire plusieurs semaines.

Vous l'aurez compris, pour éviter de vous retrouver dans une situation catastrophique, il faut vous préparer avant la crise!

Que faut-il au minimum pour survivre?

Voici quelques éléments de base qui vous permettront de survivre:

- Un plan de gestion de crise à jour;
- Des copies de sauvegarde (immuable) de l'ensemble de vos données en dehors de votre fournisseur infonuagique;
- Un plan de continuité de vos activités essentielles avec des procédures qui vous permettront de vous passer du nuage;
- Un plan de reprise informatique en cas de sinistre chez votre fournisseur (si possible, chez un autre fournisseur infonuagique).

Bien entendu, tout cela, il faut y avoir réfléchi et l'avoir mis en place AVANT la crise. Sinon, vous ne vous relèverez pas!

Le versionnage n'est pas une sauvegarde!

Une croyance populaire tend à considérer que l'infonuagique est sûre et que rien ne peut la rendre indisponible. Malheureusement, comme on a pu le constater par le passé, il n'en est rien. Le nuage repose sur des infrastructures qui peuvent elles aussi subir des sinistres et des cyberattaques.

Les fournisseurs proposent souvent de la redondance locale, zonale ou régionale. Ils ne sont toutefois pas responsables de la suppression volontaire ou involontaire des données se trouvant sur les espaces de stockage fournis au client. Les sauvegardes et les contrôles d'intégrité sont de la responsabilité du propriétaire des données.

La plupart des fournisseurs offrent un service de versionnage qui permet de conserver vos modifications un certain nombre de jours.

Au-delà de ce délai, vos anciennes versions sont supprimées définitivement.

Donc, si vous supprimez par inadvertance un fichier important, il sera définitivement perdu au bout d'un certain temps.

ADIEU MES PRÉCIEUX FICHIERS!

NORMES POUR LE NUAGE?

Obtenir une certification ou un *label* peut être un moyen pour les fournisseurs de services infonuagiques de montrer leur maturité en matière de sécurité.

La norme ISO/IEC 27017 est une norme internationale qui vise à sécuriser les services d'informatique en nuage. Elle s'adresse à tous les fournisseurs de ces services et propose des lignes directrices pour mettre en place des mesures de sécurité de l'information propres au nuage. Elle fournit des recommandations supplémentaires concernant la mise en œuvre de mesures de sécurité spécifiées dans l'ISO/IEC 27002 ainsi que des mesures de sécurité supplémentaires liées aux services infonuagiques. La norme s'adresse aux prestataires de services infonuagiques et à leurs clients et fournit des recommandations pour la maîtrise et la mise en œuvre de ces mesures de sécurité.

Aux États-Unis, le CSA (Cloud Security Alliance) délivre des certificats de sécurité pour les fournisseurs de services infonuagiques appelés CSA STAR, qui ont différents niveaux d'exigences.

En France, l'ANSSI propose une certification appelée SecNumCloud et un *label* nommé Cloud Confidence, qui reposent en partie sur la norme ISO 27001 et se complètent.

Vos sources et scripts sont-ils en sécurité?

Seront-ils accessibles en cas de besoin?
La tendance actuelle est de mettre toutes les sources des programmes chez un hébergeur infonuagique, pensant qu'ils y sont à l'abri du fait qu'ils sont versionnés et répliqués.

Oui, mais que se passera-t-il si vous supprimez « involontairement » une ou plusieurs sources et que la corbeille est vidée au bout de x jours?

Et que ferez-vous si vous n'avez plus cette source pour reconstruire votre application à la suite d'une cyberattaque?

Alors, quelles sont les principales solutions?

Voici deux stratégies qui permettent d'effectuer une reprise informatique en cas de sinistre chez son fournisseur infonuagique.

DRAAS (*Disaster Recovery As A Service*) est beaucoup utilisé dans le cadre des reprises à chaud – en fonction du type de production, on réplique les données dans le nuage (de préférence chez un autre fournisseur). Par contre, en cas de cyberattaque, il est probable que votre reprise soit elle aussi compromise.

BAAS (*Backup As A Service*) est un service de sauvegarde en ligne programmable de façon journalière, hebdomadaire, etc. Les sauvegardes peuvent être automatisées, chiffrées et stockées à différents endroits, y compris dans vos locaux. Cette stratégie est moins dispendieuse, car nul besoin d'acheter des serveurs et des licences, le tout étant mis à la disposition par le fournisseur. Cette solution est beaucoup utilisée dans le cadre des reprises à froid et en cas de cyberattaque.

Pour choisir un outil de reprise infonuagique, il faut se baser sur des indicateurs de performance tels que la durée maximale d'interruption admissible (DMIA), car plus le délai est court, plus on doit se tourner vers une solution de type DRASS. Si vous n'avez aucun problème à reprendre après plusieurs jours, vous pouvez vous diriger vers une solution BAAS. Attention! Dans tous les cas, vous devez avoir des sauvegardes immuables qui vous permettront de pallier des attaques par rançongiciel.

LES TYPES DE REPRISES INFORMATIQUES

Il existe plusieurs stratégies de reprise en cas de sinistre informatique, qui se distinguent notamment par leur délai de retour à la normale.

Reprise à froid. On dispose d'un espace vide qu'on équipe en cas de sinistre. Il faut procéder à l'achat et à l'installation de l'équipement nécessaire lorsque le sinistre survient. Cette stratégie peut prendre quelques jours ou quelques semaines.

Reprise à tiède. Cette stratégie se veut un compromis entre la reprise à froid et la reprise à chaud. On dispose d'équipement déjà en place et les données sont disponibles rapidement.

Reprise à chaud. On s'appuie ici sur la stratégie de réplication des systèmes intersites. Cette stratégie permet à l'entreprise de reprendre ses activités peu de temps après le sinistre (quelques heures au maximum).

En somme, il est nécessaire d'établir un plan de continuité des activités pour vous préparer aux imprévus qui peuvent survenir. Après avoir mis sur pied un plan de continuité en fonction du type de nuage que vous utilisez, il faut également choisir un outil de reprise informatique adéquat. Pour tirer pleinement parti de la continuité des activités dans le nuage, les entreprises doivent s'associer à des experts qui comprennent la situation dans son ensemble ainsi que les nuances subtiles de la transition vers l'infonuagique.

Alexandre Fournier

FICHE PRATIQUE DU MOIS

Construisez votre carte réflexe des 15 actions à faire en cas de cyberattaque

Ci-dessous, un exemple

1. **Signalez immédiatement le problème à votre soutien informatique** pour escalader vers la gestion de crise.
2. **Isolez les systèmes corrompus** pour éviter une propagation aux autres équipements.
3. **Déterminez l'origine de l'attaque et ses impacts** afin de corriger ce qui doit l'être et d'éviter un nouvel incident.
4. **Activez votre plan de gestion de crise.**
5. **Conservez les preuves de l'attaque** pour l'enquête.
6. **Ouvrez le registre de suivi de crise** pour conserver l'historique des actions menées.
7. **Déclenchez votre plan de continuité des affaires** pour continuer à maintenir vos services essentiels.
8. **Activez vos procédures de reprise informatique** pour reconstruire vos systèmes informatiques.
9. **Appliquez votre plan de communication de crise afin d'informer** avec le juste niveau de transparence vos clients, collaborateurs, partenaires, fournisseurs, les médias, etc.
10. **Déclarez le sinistre auprès de votre assureur** au besoin.
11. **Informez votre banque au cas où** des informations bancaires auraient été volées.
12. **Déposez une plainte auprès des autorités policières.**
13. **Notifiez l'incident auprès des autorités compétentes (CNIL, CAI) si des données personnelles** ont pu être consultées, modifiées ou détruites par les cybercriminels.
14. **Faites une remise en service progressive de vos systèmes informatiques** après vous être assuré que le système attaqué a été corrigé, et surveillez toute nouvelle attaque.
15. **Tirez des enseignements de l'attaque** et établissez des plans d'amélioration pour augmenter votre résilience.

Vous souhaitez proposer une fiche pratique?
Contactez-nous: info@crise-resilience.com

Fiche réflexe

15 actions à faire EN CAS DE cyberattaque

1. -
2. -
3. -
4. -
5. -
6. -
7. -
8. -
9. -
10. -
11. -
12. -
13. -
14. -
15. -

Offert par Crise & Résilience

SORTIE DE CRISE

Incident de disponibilité, d'intégrité et de confidentialité

La sortie de crise est fortement influencée par la nature de la crise elle-même.

Afin de décortiquer les moyens à notre disposition, nous avons découpé les incidents en 3 grands groupes, permettant ainsi de mieux comprendre les effets de chacun. Cependant, un vrai incident est généralement un mélange des 3 grands groupes, ce qui ne limitera pas les actions posées qu'à ce qui est défini dans un seul groupe.

Par Nicolas-Loïc Fortin

Conseiller stratégique

Fondateur de polysécure et cofondateur du salon de cybersécurité séQCure

Incident de disponibilité

L'incident de disponibilité est celui qui est peut-être le plus connu, le plus surveillé et généralement le plus facile à détecter. C'est la perte d'accès aux informations et aux systèmes.

Historiquement, en cybersécurité, nous faisions face à une attaque qui servait qu'à rendre indisponible par une surcharge des systèmes (DoS). C'est également l'endroit où il y a une intersection forte avec le plan de continuité des affaires, où il devra y avoir des arrimages forts pour déclencher les bons processus lors de la crise et effectuer un retour en activité le plus rapidement possible.

La sortie d'une crise de disponibilité se fait par le retour en ligne des informations et systèmes qui ont été affectés.

Cela prend la forme d'une restauration des copies de sauvegarde, le rétablissement des fonctions des systèmes qui ont été perdus ou la restauration des systèmes dans un site de relève.

Incident d'intégrité

L'incident d'intégrité est le plus intéressant, puisque c'est celui qui est le plus sous-estimé et parfois le plus difficile à détecter.

Celui-ci va de la corruption de données mécaniques, jusqu'à la modification non autorisée de certaines valeurs ou informations qui peuvent avoir des conséquences importantes pour l'organisation.

Le meilleur exemple pour représenter l'ampleur d'une crise d'intégrité, c'est la modification non autorisée du solde d'un compte de banque, que ce soit en faveur de la banque ou du propriétaire du compte. Cette modification, une fois détectée par le propriétaire du compte, va ébranler sa confiance envers l'institution. Il faut également souligner que peu de systèmes offrent une vérification d'intégrité native. Les systèmes de fichiers se limitent à la corruption mécanique. Les bases de données ont des mécanismes qui permettent de forcer l'intégrité, mais ces mécanismes ne sont pas toujours déployés sur les données critiques.

La sortie d'une crise d'intégrité est la plus complexe des trois, considérant qu'il est difficile de mesurer l'étendue de la perte d'intégrité des systèmes.

Cette difficulté est inhérente au design des systèmes qui ne mettent pas une emphase forte sur l'intégrité des données, hors des bris techniques, via la somme de contrôle. Il ne suffit pas de ramener les copies de sauvegarde, puisqu'il faut trouver les données qui ont été altérées de façon non autorisée et les rétablir à la bonne valeur. Parfois, cette valeur peut être difficile à trouver, puisqu'il faut déterminer la transaction malicieuse qui a transformé l'information.

De plus, comme cette modification est faite de façon voilée, il est d'autant plus difficile de mesurer, dans l'ensemble des systèmes, tous les endroits qui ont été modifiés de façon non autorisée.

La sortie de crise s'effectue par un retour en arrière des transactions, la vérification des historiques de transactions et de l'analyse approfondie des données pour qu'elles correspondent à leur valeur de contrôle.

En l'absence d'une valeur de contrôle, il faut reconstruire la chaine et l'historique nécessaire pour redonner la valeur d'intégrité à la donnée. Il faut également être prudent dans la portée des recherches et des corrections. Ce n'est pas toutes les données qui doivent avoir un niveau d'intégrité élevé.

La catégorisation permettra de cibler les données qui doivent absolument être corrigées de celles qui peuvent être tolérées dans un état dégradé. Cependant, des mécanismes devront s'assurer d'une convergence progressive vers des données saines et intègres.

En plus de rétablir les données dans leur état dit intègre, il faut également trouver le processus ou l'absence de contrôle qui a permis cette modification non autorisée et déployer les moyens pour que cette situation ne se reproduise.

Incident de confidentialité

L'incident de confidentialité a été mis de l'avent par les différentes lois en protection des renseignements personnels. En Europe, c'est l'arrivée du RGPD qui a mis la table sur la formalisation de ce type d'incident et surtout des règles du jeu concernant son traitement. Au moment d'écrire ces lignes, le Québec a adopté la loi 25 qui reprend l'essentiel des éléments du RGPD et le projet de loi C-27 au Canada est en cours d'étude.

La portée d'un incident de confidentialité est vaste et peut s'avérer surprenante pour certains... et peu sexy pour les gens œuvrant en cybersécurité.

Un incident de sécurité est initié du moment qu'une information personnelle ou confidentielle est vue par une personne qui n'est pas autorisée. Cela peut prendre la forme d'une lettre ou un courriel envoyé à un mauvais destinataire, en passant par une clé USB oubliée dans l'autobus, jusqu'à la fuite de données suivant une attaque par rançongiciel.

Au regard des actions à poser pour sortir de ce type de crise, nous faisons face à peu de mesures techniques, puisqu'une fois que l'information a repris son état féral[(1)], il n'est plus possible de la domestiquer de nouveau. Elle est prise dans une vie qui lui est propre. C'est d'ailleurs tout le problème de ce type de crise. Essentiellement, il faut déclarer l'incident aux autorités règlementaires lorsque de l'information confidentielle est impliquée, colmater le processus ou le système qui a permis la fuite et entreprendre des actions de réparation face aux personnes qui ont été affectées par la fuite.

[(1)]Se dit d'une espèce domestique retournée à l'état sauvage

Conclusion

La sortie d'une crise s'appuie sur les actions à poser pour corriger la situation, soit par la remise en ligne des systèmes, ou le règlement de ce qui a causé l'incident. La coordination entre les différentes facettes et expertises est importante pour garantir le succès de la sortie de crise.

Nicolas-Loïc Fortin

Intrasecure inc.

Le **SéQCure** est le plus important événement de sécurité défensive du Québec et nous revenons pour une deuxième année avec une formule hybride en offrant l'expérience en présentiel ainsi qu'à distance.

Le **SéQCure** est plus qu'un événement de sécurité, c'est un rassemblement pour tous les acteurs du milieu visant à partager nos connaissances respectives afin de bâtir, chacun à notre façon, un univers technologique plus sécuritaire.

L'expérience se décline en trois journées composées de conférences, de pointes pour les professionnels en sécurité, d'ateliers pour exposer les participants à un contexte réel des technologies de cybersécurité et d'activités, de formations de réseautage afin de favoriser une collaboration accrue entre les gens du milieu.

Vous désirez venir vivre l'expérience **SéQCure** avec nous? Les billets seront en vente sous peu! Suivez-nous sur les réseaux sociaux ou notre site web pour plus d'informations.

https://seqcure.org/

PODCAST

POLYSÉCURE

Cliquez sur l'image pour accéder au podcast

0x219 - Spécial - Infonuagique et cyber-résilience

0x210 - Spécial - PL64/L25 Formation en entreprise

0x207 - Spécial - Autopsie d'une crise - Collège Montmorency

0x206 - Teknik - Introduction au forensic

0x201 - PME - Les émotions et l'ingénierie sociale

www.polysecure.ca

SéQCure

Grand rassemblement sur La sécurité de l'information!

Le **SéQCure** est le plus important événement de sécurité défensive du Québec et nous revenons pour une deuxième année avec une formule hybride en offrant l'expérience en présentiel ainsi qu'à distance.

Le **SéQCure** est plus qu'un événement de sécurité, c'est un rassemblement pour tous les acteurs du milieu visant à partager nos connaissances respectives afin de bâtir, chacun à notre façon, un univers technologique plus sécuritaire.

L'expérience se décline en trois journées composées de conférences, de pointes pour les professionnels en sécurité, d'ateliers pour exposer les participants à un contexte réel des technologies de cybersécurité et d'activités, de formations de réseautage afin de favoriser une collaboration accrue entre les gens du milieu.

Vous désirez venir vivre l'expérience SéQCure avec nous?

Les billets seront en vente sous peu! Suivez-nous sur les réseaux sociaux ou notre site web pour plus d'informations.

👉 **https://seqcure.org/**

28 février et 1-2 mars 2023

Hotel Classique - Québec

PRÉPARER SON ENTREPRISE À LA RÉCESSION

Pandémie depuis près de trois ans. Guerre entre la Russie et l'Ukraine. Dans un tel contexte sociopolitique, on peut s'attendre à une récession imminente. Par contre, impossible de prédire de quelle façon elle touchera chaque entreprise. Chose certaine, nous pouvons tous nous y préparer afin de diminuer les risques financiers et d'atténuer son impact.

Par Guillaume Carr

Conseiller principal de l'équipe Carr

Guillaume travaille en conseil financier depuis 2015 et se spécialise avec les propriétaires d'entreprises

Maîtriser ses finances

Comprendre ses finances, c'est essentiel au succès de son entreprise. Quand on maîtrise ses chiffres, comme le budget prévisionnel et le suivi du flux de trésorerie (*cash flow*), on peut planifier de façon stratégique et s'ajuster aux aléas de la vie qu'on ne peut contrôler.

La première chose à faire pour vous préparer à une récession consiste à **redéfinir vos objectifs annuels**. Vous aviez prévu augmenter vos ventes de 15 %? Ça se pourrait que votre objectif soit plus difficile à atteindre que prévu. Vous vouliez acheter une machine qui vaut un million de dollars pour augmenter la productivité? Hum! Ce n'est peut-être pas une bonne idée.

Je vous invite aussi à **calculer votre seuil de rentabilité**, appelé aussi « point mort » ou « *break-even* ». Il s'agit du chiffre d'affaires à atteindre auquel on soustrait toutes les dépenses (variables et fixes) afin d'atteindre le bénéfice 0. Ainsi, vous devrez calculer le nombre de produits à vendre ou d'heures facturables minimum pour atteindre un chiffre d'affaires suffisant pour couvrir toutes vos dépenses.

Diminuer les dépenses

Réduire les heures supplémentaires, couper dans les dépenses non essentielles, ne pas renouveler les abonnements des plateformes et outils Web que vous n'utilisez pas (ou trop peu)… Voilà autant de façons de « couper dans le gras ».

Mais attention! Diminuer certaines dépenses, comme le budget marketing, pourrait entraîner un impact négatif à long terme.

Le marketing, la santé et la sécurité au travail, on ne touche pas à ça!

De plus, si vous prévoyez une année difficile, prenez le temps de peser le pour et le contre avant d'embaucher de nouvelles ressources.

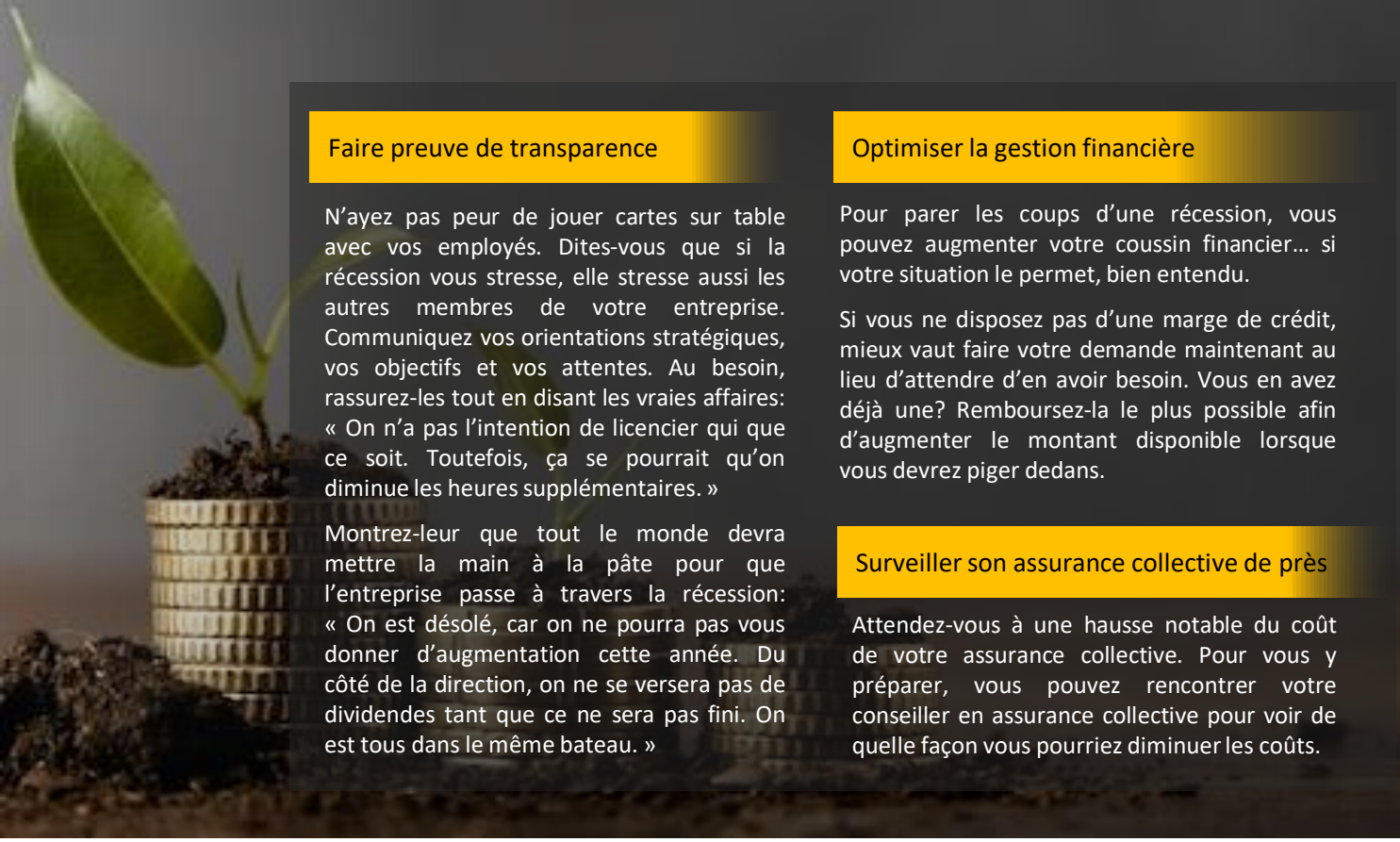
Suivre les comptes recevables de près

Le flux de trésorerie, c'est le nerf de la guerre. Il fait souvent la différence entre une entreprise en bonne santé financière et une entreprise qui frôle la faillite. Vous comprenez donc l'importance de vous assurer que vos clients paient à temps.

Pour éviter le manque de liquidités, vous pouvez exiger un dépôt à vos clients. Après tout, il n'y a rien de pire qu'un carnet de commandes plein qui fond comme neige au soleil parce que certains clients se désistent deux semaines avant le début des travaux. Si vos clients vous donnent un dépôt, ils y penseront à deux fois avant d'annuler leur commande.

En période de récession, vous devez être capable de remettre en cause tout ce que vous avez fait auparavant.

François-Henri Pinault



Faire preuve de transparence

N'ayez pas peur de jouer cartes sur table avec vos employés. Dites-vous que si la récession vous stresse, elle stresse aussi les autres membres de votre entreprise. Communiquez vos orientations stratégiques, vos objectifs et vos attentes. Au besoin, rassurez-les tout en disant les vraies affaires: « On n'a pas l'intention de licencier qui que ce soit. Toutefois, ça se pourrait qu'on diminue les heures supplémentaires. »

Montrez-leur que tout le monde devra mettre la main à la pâte pour que l'entreprise passe à travers la récession: « On est désolé, car on ne pourra pas vous donner d'augmentation cette année. Du côté de la direction, on ne se versera pas de dividendes tant que ce ne sera pas fini. On est tous dans le même bateau. »

Optimiser la gestion financière

Pour parer les coups d'une récession, vous pouvez augmenter votre coussin financier… si votre situation le permet, bien entendu.

Si vous ne disposez pas d'une marge de crédit, mieux vaut faire votre demande maintenant au lieu d'attendre d'en avoir besoin. Vous en avez déjà une? Remboursez-la le plus possible afin d'augmenter le montant disponible lorsque vous devrez piger dedans.

Surveiller son assurance collective de près

Attendez-vous à une hausse notable du coût de votre assurance collective. Pour vous y préparer, vous pouvez rencontrer votre conseiller en assurance collective pour voir de quelle façon vous pourriez diminuer les coûts.

Prévoir un plan B en cas de faillite d'un fournisseur

Disons que votre fournisseur d'aluminium vous annonce, comme ça, sans avertissement, qu'il fait faillite. Ce ne sont pas tous les fournisseurs qui ont quatorze tonnes d'acier qui traînent sur leurs tablettes et qui peuvent vous dépanner à brûle-pourpoint. Un manque de ressources matérielles peut mettre en péril votre entreprise si vous n'êtes plus en mesure d'honorer vos commandes.

Pour éviter une telle situation, vous pouvez discuter avec vos fournisseurs afin qu'ils vous donnent une garantie. Vous pouvez aussi agir en prévention en approchant d'autres fournisseurs et en validant leur capacité à vous approvisionner.

Le même principe de prévoyance s'applique si vous engagez une entreprise de placement pour votre main-d'œuvre occasionnelle. Si elle fait faillite, y a-t-il une clause dans votre contrat qui vous permet d'engager vous-même ces travailleurs?

J'en conviens, une récession, ce n'est jamais plaisant et toujours stressant. Toutefois, en s'y préparant, on peut y faire face avec résilience et agilité.

Si vous voulez des conseils personnalisés pour votre entreprise ou un accompagnement pour revoir l'ensemble de vos stratégies financières dans un contexte de récession, contactez-moi sans hésiter. Mon équipe et moi nous ferons un plaisir de vous guider.

Guillaume Carr

Soyez prêt à affronter toute crise qui pourrait menacer votre entreprise

PROFITEZ
500 $
de réduction
jusqu'au 15 février 2023

Inscrivez-vous dès maintenant à nos formations pour protéger votre entreprise contre les menaces.

www.crise-resilience.com

ÊTES-VOUS PRÊT EN CAS DE SINISTRE?

SURVIVREZ-VOUS 72 HEURES…

Panne de courant, inondation, glissement de terrain, incendie de forêt, déversement de matières dangereuses… Voilà plusieurs sinistres qui peuvent vous amener à devoir vous confiner dans votre maison ou votre entreprise, que ce soit pour quelques heures ou quelques jours. Êtes-vous prêt à réagir dans une telle situation?

Connaissez-vous vos responsabilités et celles de votre municipalité?

Par Olivier Gauthier

Président de Formation OG - AXEAZE

Lieutenant aux opérations et technicien en prévention incendie / instructeur RCR et Premiers Soins.

Petite leçon de sécurité civile 101

Au Québec, la sécurité civile repose sur le partage des responsabilités entre la population, les entreprises, les municipalités et le gouvernement du Québec. Ce partage est défini dans la Loi sur la sécurité civile.

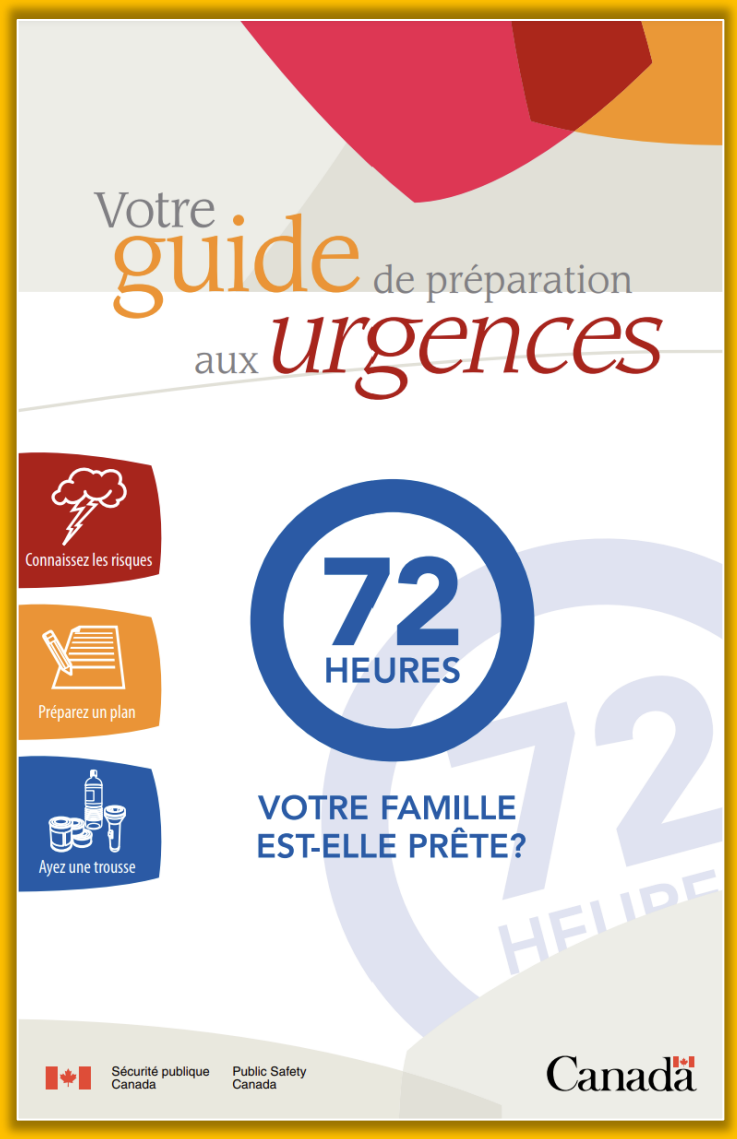
Lorsque survient un sinistre, les citoyens sont les premiers responsables de leur sécurité. Ils peuvent être soutenus par leur municipalité qui, à son tour, peut compter sur le soutien des instances gouvernementales lorsque la situation nécessite des ressources supplémentaires.

Ainsi, nous sommes tous responsables d'assurer notre sécurité, celle de notre famille (incluant nos animaux de compagnie) et la protection de nos biens. Concrètement, cela signifie que nous devons :

- Assurer nos biens (maison voiture, etc.);
- Préparer notre plan familial d'urgence;
- Avoir une trousse qui contient les articles essentiels pour être autosuffisants pendant au moins 72 heures;
- Nous renseigner, auprès de notre municipalité ou sur Internet, sur les risques de sinistre dans notre secteur et sur les mesures à prendre pour nous protéger.

De leur côté, les **entreprises** doivent se doter d'un plan de mesures d'urgence qui tient compte des conséquences que pourraient avoir leurs activités sur la population. Elles ont aussi tout avantage à prévoir un plan de continuité des opérations en cas de sinistre.

Chaque **municipalité** est responsable d'identifier les risques sur son territoire et de mettre en place des mesures pour les prévenir ou pour en minimiser les conséquences. Elle doit aussi porter assistance à la population dans les 72 heures suivant le début d'un sinistre.



SOURCE :
https://www.preparez-vous.gc.ca/cnt/rsrcs/pblctns/yprprdnssgd/yprprdnssgd-fra.pdf

Pourquoi 72 heures?

Déployer les mesures d'urgence, c'est souvent plus complexe qu'on l'imagine. Ça va bien au-delà des pompiers et des policiers qui se déplacent pour assurer votre sécurité. Le maire ou le directeur général doivent souvent prendre des décisions lourdes de conséquences. Et quand plusieurs acteurs sont impliqués, il faut coordonner les actions de chacun.

Disons que le maire de votre municipalité décide d'ouvrir un centre pour accueillir les citoyens qui n'ont plus d'électricité. Avant l'ouverture, il devra prévoir un surveillant, de la nourriture, des lits de camp… Il devra aussi penser aux besoins particuliers de certaines personnes qui seront accueillies, comme les enfants et les personnes à mobilité réduite.

Bien sûr, votre municipalité peut vous venir en aide avant les 72 heures exigées par la Loi. Et c'est toujours ce qu'elle essaie de faire. Mais les 3 premières journées, c'est avant tout VOTRE responsabilité.

Bien se préparer pour faire face à un sinistre

Chaque sinistre cause du stress et de la peur. Pour les réduire le plus possible, une bonne préparation s'impose.

Je vous conseille d'abord créer votre trousse d'urgence 72 heures que vous laisserez en tout temps dans un endroit accessible : dans le placard près de la porte d'entrée, par exemple. Assurez-vous de réunir tous les articles dans un sac à dos, un sac de sport ou une valise à roulettes. Vous ne voulez sûrement pas commencer à courir partout dans la maison, en pleine inondation, pour chercher les articles qui vous manquent.

C'est important de la revoir chaque année, car certains aliments peuvent être expirés (nourriture en conserve ou aliments déshydratés, par exemple) et les piles déchargées.

Des médicaments à ne pas oublier? Attachez un carton à votre sac sur lequel vous aurez écrit : « Ne pas oublier l'Epipen de Marjorie et le Coumadin de Stéphane ».

Dans un autre ordre d'idées, plusieurs municipalités du Québec utilisent une application pour communiquer avec leurs citoyens en cas d'urgence. Grâce à cette application, vous pourriez recevoir des alertes (météo, fermeture de route…) et avoir accès à de nombreuses informations essentielles en cas de sinistre : procédures d'urgence, conseils à suivre dans certaines situations, numéros de téléphone d'urgence, mesures mises en place pendant une crise… Pour savoir si votre municipalité utilise une telle application, je vous invite à communiquer directement avec elle.

« Est-ce que mon plan familial d'urgence est adéquat? »

« Une trousse d'urgence pour la maison, ça va, mais pour mon entreprise, qu'est-ce qu'elle doit comprendre? »

« Concevoir un plan de mesure d'urgence pour mon immeuble, ça dépasse largement mes compétences. »

J'en conviens, se préparer en cas de sinistre n'est pas si simple lorsqu'on ne s'y connaît pas. En tant que pompier, technicien en prévention incendie, premier répondant médical et instructeur en premiers soins – RCR/DEA, je peux vous accompagner dans votre démarche et vous outiller pour assurer la sécurité de votre famille et de vos employés.

Sachez que mon équipe a tous ce qu'il faut pour vous aider à monter votre trousse 72h personnalisée ou vous accompagner dans la conception de vos plans de mesures d'urgences en entreprise. Pour plus de renseignements, n'hésitez pas à me joindre par les réseaux sociaux, au travail ou visitez-nous sur internet à www.axeaze.ca ou www.formation-og.com.

Olivier Gauthier, président

AYEZ UNE TROUSSE D'URGENCE!

DE BASE :

- **Eau** — deux litres d'eau par personne par jour
- **Aliments non périssables** comme de la nourriture en conserve, des barres énergétiques et des aliments déshydratés (remplacez l'eau et les aliments chaque année)
- **Ouvre-boîte manuel**
- **Lampe de poche** à manivelle ou à piles (et piles de rechange)
- **Radio** à manivelle ou à piles (et piles de rechange)
- **Trousse de premiers soins**
- **Clés** supplémentaires pour la voiture et la maison
- **Argent comptant**, chèques de voyage et monnaie
- Documents importants de la famille, tels que vos pièces d'identité, vos documents d'assurance et vos relevés bancaires
- **Plan d'urgence** – conservez-en une copie dans votre trousse, ainsi que les coordonnées importantes

CONSIDÉREZ AUSSI L'AJOUT DES ARTICLES SUIVANTS :

- **Deux litres d'eau supplémentaires** par jour par personne pour la préparation des aliments et l'hygiène
- **Bougies et allumettes** ou briquet (placez les bougies dans des contenants robustes et ne les laissez pas brûler sans surveillance)
- **Vêtements, chaussures de rechange** pour les membres de la famille
- **Sac de couchage** ou couverture pour tous les membres de la famille
- **Articles de toilette** et articles d'hygiène personnelle
- **Désinfectant** pour les mains, papier hygiénique et sacs à ordures
- **Carte téléphonique prépayée**, chargeur pour téléphone mobile
- **Aliments et fournitures pour animaux**
- **Préparation pour nourrissons** et aliments et fournitures pour bébés
- **Activités pour les enfants**, des livres, des casse tête ou des jouets
- **Médicaments sur ordonnance**, matériel médical
- **Ustensiles, assiettes et tasses**
- **Eau de Javel** ou comprimés pour purification de l'eau
- **Outils de base** (marteau, pinces, clé, tournevis, gants, etc.)
- **Petit réchaud** à combustible et combustible
- **Sifflet** (pour attirer l'attention)
- **Ruban adhésif** électrique

Gouvernement du Canada | Government of Canada

SOURCE : https://www.preparez-vous.gc.ca/cnt/kts/bsc-kt-fr.aspx

NE JOUEZ PAS À LA ROULETTE RUSSE AVEC VOTRE ENTREPRISE!

Depuis quelques semaines, WDI.solutions compte sept nouveaux clients. Mais on doit vous avouer qu'on aurait préféré qu'ils n'aient pas besoin de nous.

Par Stéphanie Moreau

Développement des affaires | Web

Femme aux multiples talents, Stéphanie est dotée d'un sens de l'efficacité et de l'organisation hors pair.

Alerte aux arnaqueurs!

Des arnaqueurs, il y en a toujours eu et il y en aura toujours. Et quand il s'agit de s'attaquer à la vulnérabilité des gens, ce sont des champions. C'est ce qui est arrivé à nos nouveaux clients, qui se sont fait pirater leur compte personnel ET leur compte professionnel sur Facebook.

Si ce n'était que cela!

Malheureusement, aucun de ces clients n'avait de site Web – leur compte Facebook professionnel constituait leur seule vitrine professionnelle.

Résultat? Leurs clients potentiels n'avaient plus aucune façon de les trouver, de savoir qu'ils existent.

Des conséquences parfois désastreuses

Personne ne peut prévoir ce que feront les pirates informatiques lorsqu'ils auront pris le contrôle de vos comptes de réseaux sociaux. Leur créativité malveillante peut vous faire perdre votre crédibilité et votre notoriété en deux temps, trois mouvements.

Et si, en plus, vous n'avez pas de site Web, là, vous jouez carrément à la roulette russe avec votre entreprise. Votre entreprise ayant disparu du Web, votre visibilité tombe en flèche.

3 avantages d'avoir un site Web pour votre entreprise

Avantage 1

Votre site Web vous appartient, contrairement à votre compte Facebook. Plus précisément, tout ce que vous publiez sur Facebook (textes, vidéos, etc.) est seulement déposé sur la plateforme. Vous empruntez une page professionnelle; cela ne vous appartient pas. De plus, comme c'est un réseau social gratuit, pas de service à la clientèle via un service de clavardage ou une ligne téléphonique, et le délai de réponse à la page d'aide peut prendre entre 48 heures et 60 jours.

Avantage 2

Vous avez le contrôle sur votre site Web. Il ne disparaîtra jamais, à moins que vous arrêtiez de payer votre nom de domaine et votre hébergeur. Du côté des réseaux sociaux, c'est une tout autre affaire. Les algorithmes changent sans cesse. De plus, les tendances évoluent rapidement: certains réseaux sociaux qui étaient populaires il y a un an ou deux se meurent, alors que de nouveaux grimpent en popularité.

Avantage 3

Votre site Web est évolutif. Ce n'est pas vrai que pour la création d'un site Web de qualité vous devez payer 5 000 $ ou 10 000 $. Pour environ 1 800 $, l'équipe de WebDev Intégration peut vous concevoir un site de base tout aussi professionnel.

Vous pouvez ensuite décider d'y intégrer graduellement d'autres éléments comme un blogue, une messagerie instantanée (clavardage), la prise de rendez-vous, une boutique virtuelle, etc. Nous ferons évoluer votre site Web à votre rythme, en fonction de vos besoins et de votre budget.

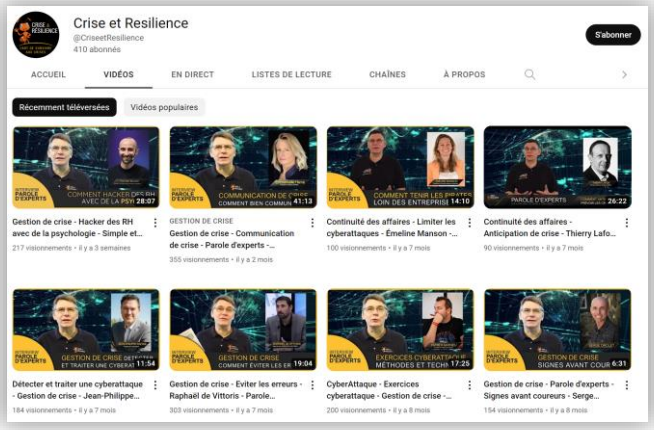
En terminant, nous vous rappelons que les réseaux sociaux représentent un outil de marketing essentiel au succès de toutes les entreprises. Toutefois, ils doivent être complémentaires à votre site Web, et non l'inverse. À ce sujet, nous vous invitons à lire l'article Site Web et réseaux sociaux: le mariage de l'année!

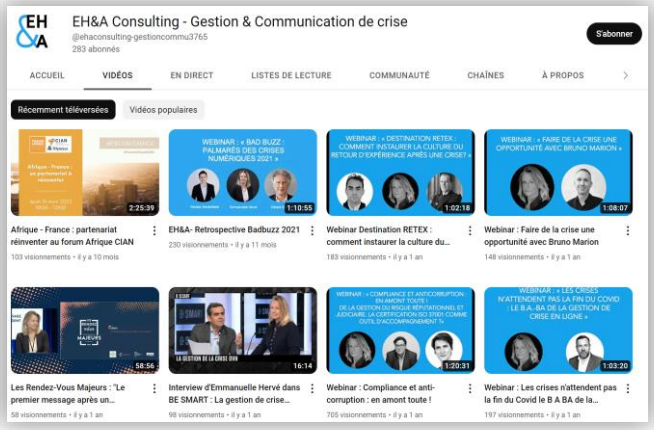
Des questions? Des commentaires? Communiquez avec nous dès maintenant.

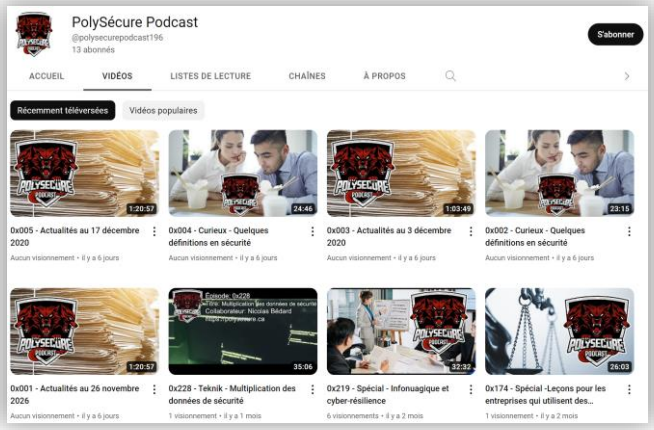
Stéphanie Moreau

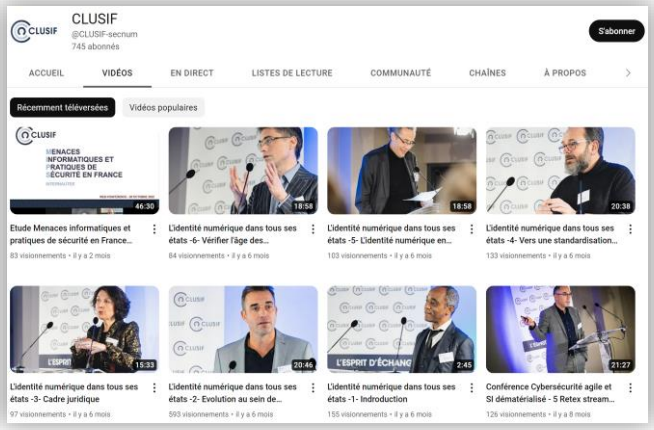
LES MÉDIAS DU MOIS — Des ressources en ligne pour apprendre plus!

Il est important de s'informer et de se former régulièrement pour être en mesure de gérer efficacement les situations de crise et de renforcer la résilience de son organisation. N'hésitez pas à consulter ces sites et à regarder ces vidéos pour approfondir vos connaissances et vous tenir à jour sur les dernières tendances en matière de gestion de crise et de résilience organisationnelle.









Vous souhaitez apparaître ici? Contactez-nous: info@crise-resilience.com.

Interview

Parole d'experts

YouTube Visitez notre chaine

Crise et Resilience
@CriseetResilience
400 abonnés

ACCÉDEZ GRATUITEMENT À PLUS DE 50 VIDÉOS SUR :

la gestion de crise, la continuité des affaires, la reprise informatique

LES ACTIVITÉS À VENIR — Conférences, ateliers, formations et plus!

D'ici le prochain numéro du magazine Crise & Résilience en avril, nous vous proposons plusieurs activités, qui vous sont offertes par nos annonceurs. Vous trouverez des conférences, des ateliers, des formations, des salons et plein d'autres activités.

Le **SéQCure** est le plus important événement de sécurité défensive du Québec et nous revenons pour une deuxième année avec une formule hybride en offrant l'expérience en présentiel ainsi qu'à distance.

Le **SéQCure** est plus qu'un événement de sécurité, c'est un rassemblement pour tous les acteurs du milieu visant à partager nos connaissances respectives afin de bâtir, chacun à notre façon, un univers technologique plus sécuritaire.

L'expérience se décline en trois journées composées de conférences, de pointes pour les professionnels en sécurité, d'ateliers pour exposer les participants à un contexte réel des technologies de cybersécurité et d'activités, de formations de réseautage afin de favoriser une collaboration accrue entre les gens du milieu.

Vous désirez venir vivre l'expérience **SéQCure** avec nous? Les billets seront en vente sous peu! Suivez-nous sur les réseaux sociaux ou notre site web pour plus d'informations. **https://seqcure.org/**

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

ADRESSES PROFESSIONNELLES

Elles pourraient vous être très utiles.

Les professionnels travaillant en lien avec la résilience organisationnelle, la gestion de crise et la cybersécurité sont des experts formés pour gérer des situations d'urgence et prévenir les risques qui pourraient avoir une incidence sur votre entreprise. Ils sont indispensables pour les entreprises soucieuses de protéger leur activité et leur réputation. Voici quelques adresses de professionnels qui pourraient vous être utiles:

CRISE & RÉSILIENCE

Notre mission
Gestion & simulation de crise – Continuité des affaires – Formation – Coaching – Sensibilisation

Site Web
www.crise-resilience.com

CYBERSWAT

Notre mission
Vous protéger des pirates, peu importe la taille de votre entreprise

Site Web
www.cyberswat.ca

EHA consulting

Notre mission
Gestion & simulation de crise – communication de crise – Reconstruire après la crise

Site Web
www.eha-consulting.com

INTRASECURE INC.

Notre mission
Nous travaillons à protéger vos informations précieuses.

Site Web
www.intrasecure.ca

AXEAZE

Notre mission
Procurez-vous le matériel nécessaire pour faire face à toutes les situations!

Site Web
www.axeaze.ca

WDI.SOLUTIONS

Notre mission
On met le web à votre portée

Site Web
www.wdi.solutions

Équipe CARR

Notre mission
Vous travaillez fort pour votre argent, il est temps de le faire travailler pour vous!

Site Web
https://conseiller.groupeinvestors.com/fr/guillaume_carr

Vous souhaitez apparaître ici? Contactez-nous

info@crise-resilience.com

Vous souhaitez apparaître ici? Contactez-nous

info@crise-resilience.com

Vous souhaitez apparaître ici? Contactez-nous

info@crise-resilience.com

Vous souhaitez apparaître ici? Contactez-nous

info@crise-resilience.com

Prochain numéro le 3 avril 2023

Abonnez-vous pour le recevoir

www.Crise-Resilience.com/magazine