Faire de la cybersécurité une valeur ajoutée pour l'entreprise

Anne DORÉ
Co-auteure
« Cybersécurité – Méthode de Gestion de Crise »
Fondatrice - ADHEL

La crise cyber est une nouvelle certitude que les entreprises doivent intégrer dans leur gestion des risques. Même les entreprises déjà victimes, ne sont pas à l'abri d'une nouvelle attaque et celles qui ont réussi jusqu'à maintenant, à passer à travers les mailles du filet, n'ont qu'à bien se préparer. Elles n'y échapperont pas.

La digitalisation de l'économie et des processus métier au sein des entreprises, dans un contexte de pandémie mondiale, a mis en exergue les faiblesses structurelles en matière de sécurité numérique et l'absence de préparation de nombreuses organisations, notamment celles non soumises à des contraintes règlementaires.

Pour autant, nombre d'entreprises cherchent à se rassurer et pense pouvoir gérer une crise cyber en se fiant à leurs expériences acquises lors de précédentes crises, la dernière étant celle de la Covid 19. Il faut néanmoins rappeler que la cybersécurité n'est pas une crise comme les autres !

La crise cyber résulte d'une action malveillante ayant la volonté de nuire à l'organisation. N'importe quelle organisation – publique ou privée –quel que soit son secteur d'activité ou sa taille, peut se retrouver de manière frontale face à des demandeurs de rançon ou à devoir faire barrage à des cybercriminels, paraétatiques ou activistes cherchant par tous les moyens à pénétrer au cœur du système d'information.

Les spécificités de la crise cyber résident dans le fait qu'on se retrouve face à un adversaire organisé, malveillant et souvent professionnel et que les conséquences ne sont pas uniquement informatiques. Elles sont humaines si la cible est un CHU, économiques, financières, industrielles et, ou informationnels quand une attaque génère l'arrêt d'une chaine de production ou nuit à la réputation de l'entreprise en prenant par exemple le contrôle d'un vecteur de communication comme un site internet. La crise cyber est donc un risque métier qu'il faut appréhender, gérer et prévenir.

Elle exige donc de la part des organisations une réaction rapide, pertinente et efficace. La réaction apportée varie selon la nature, l'envergure et l'impact des risques générés et les scénarios de crise préalablement définis.

La complexité et le besoin de réactivité sont telles des réponses selon les risques métiers encourus et la nature de la crise. L'anticipation et la

préparation sont des vecteurs clés de réussite dans la gestion de crise. Elles auront aussi pour mérite d'en limiter l'impact et d'éviter une crise dans la crise.

Dans la « Méthode de gestion de crise[1] » , nous décrivons comment cette préparation passe par un apprentissage permanent et itératif s'appuyant sur 2 cycles : le cycle nominal consistant à anticiper, préparer et prévenir la crise et le cycle de gestion de crise. Ces deux cycles interviennent à des moments différents, mais sont interdépendants et ont pour objectif commun d'améliorer en permanence la capacité de résilience de l'organisation.

Construire des organisations résilientes pour prévenir les attaques et limiter leurs impacts

La nature du risque et les objectifs déclinés en risque métier propre à chaque entreprise font que la préparation et la gestion d'une crise de nature cyber est complexe.
Une approche proactive est indispensable : les attaques sont ingénieuses et ciblées, aucune entreprise ne peut se considérer comme invulnérable. Il faut ainsi préparer les scénarii et adopter un plan de gestion de crise cyber qui guideront le tempo opérationnel.
Le premier cycle est vertueux. Il amène chaque organisation à mettre en œuvre un dispositif lui permettant de se préparer dans les meilleures dispositions pour éviter, et si nécessaire s'apprêter à l'affronter. La clé de voute de cette préparation réside dans la capacité pour chaque entreprise à déterminer les actifs, « joyaux de la couronne », qui doivent être protégés et à imaginer des scénarii selon le type et la nature de la crise.
Pour ce faire, l'entreprise doit en premier lieu s'assurer de la bonne mise en place de la gouvernance de la sécurité de son système d'information avec sa politique et son système de management approprié. Il convient aussi de pouvoir adresser les enjeux de prévention, de détection et de réponse à incidents.
Le second cycle est déclenché dès qu'un ensemble d'éléments fait que l'organisation ne peut plus ignorer la situation de crise, ou que la survie de celle-ci est en jeu. C'est le processus de gestion de la crise.
Le cycle de gestion de crise, préalablement défini dans le cycle nominal, vise à déterminer la démarche à suivre en cas de crise. La priorité absolue est de contenir l'attaque pour préserver les ressources de l'entreprise et pouvoir basculer au plus vite en phase de remédiation afin de limiter au maximum les conséquences négatives.
La complexité et la taille de la structure de l'organisation de gestion de crise dépendent bien évidemment des caractéristiques de l'entreprise. D'une manière générale, elle est constituée non pas d'une cellule, mais de plusieurs cellules de gestion de crise. L'idée est de scinder l'entité qui décide des entités qui exécutent tout en s'assurant d'une bonne communication et coordination entre les entités. Dans les petites entreprises, la structure se limitera à une cellule décisionnelle en charge du pilotage et de plusieurs cellules opérationnelles en charge de l'exécution.
La mise en place d'un plan de gestion de crise réduit de manière significative les risques associés et permet d'en atténuer l'impact, tout en garantissant un retour accéléré au mode nominal dans les meilleurs délais.
Mais au-delà de cette approche vertueuse, chaque crise cyber réelle ou simulée doit être perçue comme une opportunité d'accélérer la transformation de l'entreprise pour améliorer son organisation, ses processus et développer son capital humain.

[1] https://www.va-editions.fr/cybersecurite-c2x35356757

Construire une organisation cyber-résiliente ou comment faire de la cybersécurité un avantage compétitif

La crise Covid et les nombreuses discussions sur le retour au « monde d'avant » illustrent que la probabilité d'un retour à la « normal » est quasi nulle. Autre constat, si les confinements successifs ont impacté toutes les sociétés, il en ressort que celles d'entre elles qui en ont profité pour accélérer la digitalisation de leur processus métier, la mise en place du télétravail ou par exemple, l'accès à de nouveaux marchés via l'utilisation d'internet ou de « marketplace » sont ressorties gagnantes.

Dans une étude publiée en avril 2020[2], le cabinet de stratégie BCG démontre que les entreprises les plus rentables depuis la crise de 2008, indépendamment du pays ou du secteur d'activité, ont traversé quatre phases : « la gestion de la turbulence, la stabilisation, la reprise et la poursuite de l'accélération ».

C'est pourquoi chaque crise, exercice de crise doit être une opportunité pour l'entreprise pour renforcer sa résilience cyber et identifier les améliorations à apporter au sein de son organisation, ses processus et sa gestion des RH afin d'être plus forte, plus innovante ou se transformer plus rapidement.

Dans son livre « Antifragile : Les bienfaits du désordre », Nassim Nicholas Taleb va d'ailleurs plus loin et affirme que les entreprises ne devraient pas être résilientes, pour éviter de revenir dans une situation d'avant crise. Les entreprises devraient être « anti-fragiles », à savoir qu'en situation « post crise », elles doivent être différentes de celle avant la crise, différentes de la situation nominale d'avant crise.

L'apprentissage permanent est donc un des maîtres mots de la gestion de crise. Apprendre de ces expériences « simulées » ou réelles pour se renforcer et développer la résilience de l'entreprise est un facteur clé de réussite pour mieux gérer la prochaine crise et sensibiliser encore plus l'ensemble des collaborateurs, dirigeants inclus.

Cet apprentissage et la mise en place de ce dispositif vertueux résultent de l'efficacité et l'opérabilité du retour d'expérience (RETEX) à chaud et froid des exercices de crise et des crises elles-mêmes. Il en ressort alors des améliorations stratégiques ou opérationnelles (RH, équipements, outils, soutien, organisation…) qui devront être intégrées dans la gouvernance de l'entreprise et celle de la gestion de crise. Par ailleurs, une crise est une opportunité de renforcer une image de marque, d'apporter une autre dimension à la gestion des ressources humaines ou de renforcer la relation avec ses partenaires et ses clients.

La construction d'une organisation résiliente est donc source de valeur ajoutée et contribue à améliorer la performance économique et financière de l'entreprise.

Intégrer la cybersécurité dans la gouvernance de l'entreprise

Force est de constater une nouvelle fois que la cybersécurité et la construction d'une organisation cyber résiliente requièrent une approche transversale et 360°. Elles impactent la stratégie et l'organisation de l'entreprise. `

[2] https://www.bcg.com/fr-fr/publications/2020/crisis-spark-transformation-renewal.aspx

Si une crise cyber peut négativement impacter le bilan de l'entreprise, il peut aussi avoir des conséquences pour les dirigeants qui pourraient se voir reprocher par les investisseurs d'avoir négligé ou sous-estimé l'ampleur et les conséquences d'une telle crise. A contrario, une bonne gestion de crise cyber ne pourra que renforcer l'image et la réputation de l'entreprise au sein de l'écosystème et des investisseurs.

Le directeur général et les dirigeants de l'entreprise ont donc tout intérêt à s'impliquer dans la stratégie et la mise en œuvre de la cybersécurité de l'entreprise et plus encore celle de la gestion de crise. La cyber résilience est un volet à part entière de la gouvernance de l'entreprise. Il y va de sa réputation et de sa capacité à évoluer en permanence pour s'adapter aux besoins du marché et aux menaces. Elle constitue une véritable opportunité pour accélérer la mise en œuvre de la stratégie d'entreprise.