Crise sanitaire crise cyber : différences ou similarités ? Quels enseignements en tirer ?

Nous, Didier Spella et Delphine Chevallier, nous sommes rencontrés grâce au Général Marc Watin-Augouard au FIC en Janvier 2020. A la croisée de nos expertises, nous vous proposons une mini-série d'articles co-écrits ensemble afin de répondre à ces questions. Voici le déroulé complet.

La crise actuelle nous plonge dans un état unique qui pourtant n'est pas le premier et ne sera sûrement pas le dernier.

Notre génération a connu de nombreuses crises économiques et financières. Avec l'épidémie du virus Covid-19, elle traverse sa première crise sanitaire de grande ampleur à laquelle elle semblait bien mal préparée.

Comme celle-ci a un impact direct sur notre santé, elle est prise en compte par l'ensemble des dirigeants de la planète. Depuis plusieurs mois, de nombreuses communautés d'expertise alertent sur d'autres types de risques auxquels nous sommes sans nul doute aussi mal ou peu préparés : les risques liés aux changements climatiques, les risques liées au développement du numérique pour ne citer qu'eux.

Si ces crises sont inévitables, soyons réalistes, l'objectif des dirigeants doit être d'en minimiser les impacts afin que la société puisse continuer à fonctionner même en mode dégradé. Une activité normale devra bien pouvoir reprendre au bout d'un certain temps. On parle alors de Résilience - valeur caractérisant la résistance au choc d'un métal.

Prenons donc ces deux crises, sanitaire et cyber, la deuxième exploitant aujourd'hui malheureusement les failles engendrées par la première. Quelles sont alors leurs similarités et ce qui pourrait bien les différencier ?

Commençons à apprendre des similarités de ces 2 crises.

Les crises sont très rarement purement nationales, ne respectant aucune frontière et finalement finissent par nous rapprocher.

Dans un monde de plus en plus globalisé, les risques n'ont pas de frontières : les virus et les microbes font fi des limites géographiques établies par les hommes. Avons-nous vraiment tous conscience qu'il en va de même pour les logiciels malveillants utilisant des réseaux numériques ? On constate de plus que ces crises effacent des différences : Nord / Sud, démocratie/régime autoritaire, pays émergents/économie mature.

👉 Sanitaire ou cyber, nous sommes et serons tous touchés de la même manière.

Leurs origines sont très difficiles à identifier

Dans n'importe quelle crise, au moment de son déclenchement, nous avons besoin d'en connaître l'origine. La recherche du patient 0 pour une crise sanitaire a son équivalent en cas de crise cyber. 👉 Saviez-vous que la recherche de la machine infectée en premier est primordiale pour identifier les cyber criminels responsables de la malveillance ? Une fois identifiée, il faudra veiller à déconnecter cette machine du réseau tout en la laissant sous alimentation électrique afin de conserver les traces en mémoire.

Peut-être est-ce une complexité additionnelle dans le monde cyber où il y est plus facile d'effacer les traces originelles que dans le monde biologique.

Elles sont brutales et nous surprennent dans notre impréparation chronique

Le caractère brutal du déclenchement et l'enchaînement des événements caractérisent l'entrée en crise. Il est toujours facile après coup de pointer des signes avant-coureurs que nous aurions dû identifier bien plus tôt pour mieux être préparés. Mais c'est plutôt la minimisation des cygnes noirs ou notre excès de confiance, des biais cognitifs pourtant bien connus, qui nous entraînent vers les crises.

Et c'est bien le cas en cybersécurité : de nombreux indices nous signalent une montée des risques. Hélas, combien d'entre nous les prennent en compte ? 👉 Dans quelques mois, le cyberespace va-t-il nous jouer le mauvais tour de nous projeter dans une situation similaire ? La conséquence pour les organisations, qu'elles soient publiques ou privées, sera à nouveau la paralysie totale de leurs activités, suivi de difficultés majeures de remises en route et de nouvelles pertes financières significatives.

Quelles conséquences pour une organisation déjà très fragilisée financièrement par la crise sanitaire qu'elle traverse si elle avait à affronter ensuite une crise cyber ?

La crise que nous traversons, a un impact total sur l'ensemble des individus et nous le sentons en ce moment, peut nous faire basculer dans une crise sociétale et de valeurs. Il en est de même pour une crise cyber.

On pourrait croire qu'une crise cyber n'aura des conséquences que dans le monde virtuel. Cependant des individus seront bel et bien impactés, comme dans d'autres types de crise. Leur vie pourrait même être mise en danger comme le

montre les exemples malheureux de cyberattaques directes sur le CHU de Rouen ou plus récemment celui de la Pitié Salpêtrière. Il peut aussi en être de même, avec des services de santé et de soins victimes collatérales de défaillances chez un de leur prestataire ou une prise de contrôle malveillante d'un outil connecté d'un véhicule par exemple.

De tout temps, les crises (guerre, catastrophe, crack boursier), ont bousculé notre hiérarchie des besoins nous ramenant à nos fondamentaux des deux premiers niveaux de la pyramide de Maslow : besoins physiologiques et besoins de sécurité. Ce qui nous paraissait nécessaire jusqu'alors devient superficiel. Il en va de même pour la hiérarchie de nos valeurs.

La crise sanitaire a aussi cela de commun avec une crise cyber. Qu'avons nous entendu de celles et ceux, dans les organisations qui ont traversé une crise cyber, tenir ses propos : "nous voici revenu au papier et au crayon" , "quel retour en arrière !", "la priorité des activités, c'est de servir nos clients et d'expédier les commandes", "notre priorité à tous, c'est de se mobiliser pour restaurer le parc informatique"...

D'autre part, les solutions correctives mises en place, dans les deux cas, peuvent faire appel à des éléments difficiles à accepter en temps normal, comme des restrictions de libertés, la remise en cause de certaines exigences techniques, de valeurs culturelles, voire morales. Cette situation nous questionne quoiqu'il arrive : existe-t-il d'autres moyens ? Peut-on accepter de se remettre en cause sur une période donnée ? Qu'en est-il du transfert de responsabilités sur l'autorité centrale vs responsabiliser les équipes locales ? Que sommes nous prêts à tolérer pour éviter un creusement des inégalités ?
Par exemple, en cas de crise cyber, nous pourrions être amenés à utiliser des outils moins performants ou ne répondant pas aux exigences de l'organisation en temps normal, voire, pour pouvoir continuer à travailler, aller nous procurer du matériel directement au magasin du coin sans passer par le processus achat. L'ordre hiérarchique habituel peut subir lui aussi des modifications profondes afin de répondre plus rapidement aux besoins du terrain.

Dans tous les cas, nous sommes confrontés à un questionnement profond : à quoi je sers, à quoi sert mon travail, mon positionnement dans la société / dans l'entreprise ? quelles initiatives dois-je ou puis-je prendre ?

Face à l'impréparation, le traitement de la crise nécessite des investissements colossaux.

Comme pour cette crise sanitaire, une crise cyber fait face aux mêmes défis : dois-je m'y préparer ou pas ? Avec quel niveau de priorité ?
Lorsqu'elles se produisent, ne pas s'y être préparé nécessite la mise en place d'outils et de moyens exceptionnels au sens large. Nous nous en rendons bien compte actuellement. Cette mise en place n'en est que plus onéreuse, de par la rareté ou le degré d'urgence à se procurer les ressources nécessaires pour reprendre le contrôle.
Notons de plus, que l'efficacité des dispositifs n'est pas toujours reconnue et peut prêter à critique puisque l'on agit en mode "urgence". Celle-ci ne sera appréciable qu'à l'issue de la crise, avec du recul, et en fonction du résultat obtenu.

Finalement vaut-il mieux s'éduquer à vivre avec les risques ? Ou trouver un juste équilibre entre logique financière et risque acceptable ?

Les organisations face à la crise proposent des solutions incertaines et qui incitent à la critique.

Lorsque l'on rentre en crise (celles et ceux qui ont traversé une crise cyber le savent bien), les décisions se prennent logiquement dans l'urgence. Face à l'incertitude et dans un environnement où nous avons perdu la plupart de nos repères, il n'y a pas une stratégie, mais plusieurs. L'enjeu est bien dès lors, dans la capacité à décider à l'instant t en fonction des données connues et des moyens dont on dispose. Que communiquer à ses clients alors que l'on n'est pas encore en mesure d'évaluer le volume de données potentiellement piratées ? Quelles instructions transmettre à ses collaborateurs alors que l'on est dans l'incapacité de définir une date précise de remise en route des systèmes ? ...

Nous ne sommes pas toujours aidés dans ces prises de décisions, ayant bien souvent affaire à des “sachant”, utilisant un « vocabulaire savant” où tout à chacun n’y comprend pas forcément grand-chose.

La solution ne se trouve-t-elle pas alors dans l’alignement derrière un leader ?
Le temps du débat doit laisser place à celui de la collaboration et de la conscience collective.

Ces crises font appel à des notions de résilience et de résistance identiques. Par résilience il s’agit de notre capacité à reprendre une activité normale. Pour la résistance il s’agit de traverser les événements à “moindre mal”.

Quoiqu’on y fasse, après l’entrée en crise, nous traversons tous, individuellement et collectivement, les mêmes phases émotionnelles, mais à des rythmes différents. Se remettre en route en sortie de crise dans un nouveau contexte et s’adapter, est plus ou moins difficile. En effet se synchroniser avec des nouveaux enjeux, encore plus lorsque l’environnement est incertain voire inédit, demande du temps et de l’énergie.
Il en va de même lors d’une crise cyber. En cas de destruction ou de dysfonctionnement grave des systèmes numériques, nous sommes alors obligés de nous mettre dans une forme de confinement technologique (résistance). Par la suite, la reconstruction de ces systèmes permet une remise en route (déconfinement). Nous retrouvons alors un mode de fonctionnement opérationnel à peu près “normal”.

Enfin, en temps de crise, les réactions des individus sont similaires. Trop souvent nous ne nous sentons pas concernés, que ce soit dans la phase de prévention, lors du déclenchement, et parfois même aussi au point culminant de la crise.

Dans les deux cas (crise sanitaire et cyber), nous avons à faire à un ennemi invisible et « inconnu ».
L’infection est toujours silencieuse : période d’observation, incubation, élévation de température. Savez vous qu’il en va de même en cas d’infection cyber ? Bien souvent, le logiciel malveillant, le virus s’installe discrètement sur votre machine. Vous ne le voyez pas. Une activité anormale du processeur (ainsi que du réseau) est néanmoins un signe avant-coureur permettant de détecter sa présence.
De même, la plupart des individus peut se croire “immunisé” : pourquoi serai-je touché alors que je suis en bonne santé? Avec son équivalent en matière cyber : qui pourrait m’en vouloir ? Je n’ai rien à cacher, mes données n’ont pas de valeur.
La crise actuelle que nous traversons nous apprend beaucoup. Prenons le temps d’en tirer tous les enseignements personnels et organisationnels. Il nous sera alors plus facile d’affronter une potentielle crise, même cyber. Cependant, ne nous leurrons pas : en matière de crise cyber, nous manquons encore d’expérience collective. Nous identifions et anticipons de véritables différences que nous devons appréhender dès maintenant.

La première différence la plus évidente est sans doute la vitesse de propagation.

Une cyberattaque est mondialement quasiment instantanée, que ce soit dans la phase d’observation (installation d’un logiciel espion s’implantant sur l’ensemble des machines en quelques minutes) ou dans la phase de déclenchement (exécution du logiciel destructeur).

Des organisations internationales victimes de l'attaque NotPetya ont rapporté qu'il a fallu moins de 90 minutes pour détruire ou mettre à l'arrêt la totalité de leur infrastructure numérique.
Cette violence brutale, impactant les individus et les activités, est encore trop négligée par les organisations qui se préparent à ce type de crise.

La deuxième réside peut-être dans le comportement criminel qui n'a qu'un objectif : mettre à mal les systèmes d'une organisation afin d'en tirer un profit pécunier.

Les attaques cyber ont toujours une origine malveillante, qu'elles visent à la destruction des systèmes ou à utiliser les outils numériques à des fins d'escroquerie. Leur finalité est toujours la même : obtenir un gain financier.
Ce constat amène les organisations à investiguer de nouveaux modes d'actions pour se prémunir :

1. surveiller en temps réel le fonctionnement et les performances des systèmes numériques,
2. anticiper les malveillances potentielles d'origine interne ou externe,
3. réagir techniquement, sur le plan judiciaire et en matière d'assurance,
4. signaler les incidents aux instances concernées afin de contribuer à la protection générale.

Une troisième différence apparaît dans le fait que le cybercriminel peut choisir sa ou ses victimes, contrairement à la maladie virale.

La perception commune pour une maladie reste qu'elle touche de manière aléatoire les individus. Même si nous sommes aussi conscients que certains d'entre nous sont plus susceptibles que d'autres d'être contaminés, pourquoi l'un est contaminé et pas l'autre garde une forme de mystère. De même les conséquences de la maladie sur les organismes ne sont pas toujours de même niveau.
Cependant en matière de virus informatique force est de constater que la contamination et l'impact sont identiques sur toutes les infrastructures. Les conséquences sur les systèmes sont donc bien plus radicales et homogènes. Peut-être un seul côté positif : en matière cyber les dommages sont sur les machines et non sur le corps humain. Même si par ricochet, nous l'avons évoqué précédemment, il peut y avoir de graves conséquences sur la vie humaine.
Restons vigilants sur ce point : le développement rapide de l'intelligence artificielle et de la robotique commence à remplacer des gestes manuels (notamment en chirurgie). Nous pouvons nous interroger sur les conséquences encore plus dramatiques d'une attaque cyber sur ce type de matériel si nous perdons le contrôle manuel de certaines tâches ou notre faculté de raisonnement. Il apparaît encore plus essentiel aujourd'hui de conserver et cultiver notre esprit critique afin de challenger en permanence ces outils facilitateurs.

La courbe d'expérience est un autre point de différences.

La maladie, les pandémies (la peste, H1 N1, la grippe saisonnière, espagnole) sont dans notre adn collectif depuis nos origines. Nous avons tous été un jour malade et nous en connaissons parfaitement les conséquences très intimes (souffrance, désagrément, effets secondaires…).
Il n'en va pas de même pour des crises cyber pour laquelle à ce jour, même si elles sont en augmentation, nous refusons d'appréhender encore les impacts et conséquences qu'elles auraient sur nos activités.

Serions-nous dans une forme de déni ? Si lorsque nous avons de la fièvre, nous allons naturellement chez le médecin, il en va tout autrement quand nous recevons des mails frauduleux. Savez vous qu'un mail de ce type est une forme d'attaque ? Qui d'entre vous les signale systématiquement* ? Qui met en place dans la foulée des actions de protection ou de vérification de son système ?

De plus, nous avons vu qu'en cas de crise sanitaire, les actions qui nous sont demandées, même si elles nous dérangent parfois, sont bien comprises et déjà ancrés dans nos pratiques. En cas de crise cyber, comment réagirions nous ? Connaissons-nous les bons gestes essentiels en cas d'attaque ? Quelles seraient nos solutions de repli si nos outils numériques étaient à l'arrêt ? Comment conserver les preuves de l'attaque ?
Nous voyons bien par ces questions tout le chemin qu'il nous reste collectivement à parcourir afin de ne pas être démuni face à une pandémie cyber potentielle.
Avons-nous conscience de l'explosion du nombre d'attaques cyber ces dernières semaines ? Est-ce suffisant pour que nous commencions enfin à acquérir ces nouvelles pratiques pour bien nous protéger ?

* pour signaler les mails frauduleux, ayez le réflexe signal-spam !

Cela vous surprendra peut-être : un attaque cyber a toujours une origine humaine.

Derrière toute attaque cyber, qu'elle soit directe, à partir de réseaux d'ordinateurs* ou qu'elle utilise de l'intelligence artificielle, il y a toujours forcément un individu ou un groupe d'individus qui a construit la stratégie et les moyens par lesquels les attaques vont se déclencher. Aujourd'hui, sauf dans le contexte de guerre chimique, derrière une contamination virale sanitaire, il n'y a pas d'acteurs humains directs.

Dans notre subconscient, il est intéressant de constater que, alors que l'humain reste à l'origine de la construction du risque cyber, nous nous y sentons presque plus démunis que face à un risque sanitaire. Il est paradoxal de vivre avec cette croyance que l'attaque cyber est incontrôlable et imprévisible alors que nous sommes en mesure d'en maîtriser tous les mécanismes et les effets. FInalement, se prémunir des risques cyber passe par une meilleure compréhension des technologies utilisées : tout est une question d'éducation et d'enseignement pour tous,

Cependant, force est de reconnaître que le champ est vaste pour mettre à niveau nos comportements. Nous sommes toujours dans une phase de développement où des incidents cyber peuvent encore avoir malheureusement pour origine une mauvaise manipulation sans intention malveillante.

En conclusion, qu'elles soient sanitaires ou cyber, ces crises replacent l'individu au centre de nos préoccupations comme acteur unique indispensable. Il est le premier élément de toutes mesures de protections. Pourquoi avons-nous tendance à envisager le monde cyber que sous le seul angle du confort et de l'ajout de pléthore de fonctionnalités ? Les produits et services fournis n'amènent pas forcément un véritable progrès sociétal porteur de sens et de valeur. Ils créent plutôt une illusion de confort. Ces solutions, en nous noyant dans des "outillages" plus ou moins utiles, nous détournent des questions essentielles : où sont nos données ? que fait-on avec ? qui contrôle l'accès à nos activités ? quelles sont nos vulnérabilités ? Et encore bien d'autres questions liées à notre protection intrinsèque, dans le monde cyber comme dans notre vie quotidienne.

Nous devons arrêter d’être de simples utilisateurs passifs. Quel que soit notre niveau de connaissance et compétence actuelles, il est temps que nous devenions tous véritablement acteurs du monde cyber. Ne le laissons pas uniquement entre les mains de quelques ‘élites’ savantes en matière de technologie.

Le temps est venu de nous impliquer et de nous engager au quotidien pour changer dès à présent nos pratiques numériques. Intégrer de nouveaux comportements, anticiper les risques, rester dans le questionnement, nous permettra de traiter les crises cyber plus sereinement. Comme la nature sait si bien le faire, se réinventer, savoir se reconstruire sont aussi des sources formidables d’inspiration, d’énergie et de progrès collectif.

A très bientôt pour de nouvelles réflexions,

* un botnet est un réseau d’ordinateurs infectés par un logiciel malveillant spécialement configuré pour mener des attaques de masse

Delphine Chevallier, est fondatrice de Thalia NeoMedia éditeur du livre "Cyberattaque : Plongez au coeur du blackout!".. Elle définit des parcours personnalisés pour sensibiliser les utilisateurs en cybersécurité

Didier Spella, est président de Mirat di Neride, co-fondateur de Charente-Maritime Cyber Sécurité (CMCS)