



GUIDE CYBER RÉSILIENCE

LA GESTION DE CRISE

Par Cédric CARTAU

SOMMAIRE

CYBER RÉSILIENCE

0.7

LES CYBERATTAQUES

1. INTRODUCTION

P.5

2. DÉFINITION DE LA CRISE

P.6

3. LES FONDAMENTAUX

P.7

3.1 Le concept de modes mentaux

3.2 Les facteurs humains

3.2.1 Origine des accidents

3.2.2 Stress et performances

3.2.3 Considérations additionnelles

3.3 Les éléments d'une crise

3.3.1 Points communs à toutes les classes de crise

3.3.2 Spécificités des crises cyber

3.4 Les étapes de la gestion de crise

3.5 Aux confins de la crise

Approche métier : Point de vue de CrowdStrike

P.14

4. AVANT LA CRISE : LA PRÉPARATION

P.17

4.1 Visions globales

4.1.1 La vision darwinienne

4.1.2 La vision risques

4.1.3 La vision mode mental

4.1.4 Vision Deming

4.2 Se préparer : le BUILD du PDCA

4.3 Spécificités du PLAN dans la santé

4.4 Les livrables du BUILD

4.4.1 Gouvernance globale

4.4.2 Dispositions par MOA

SOMMAIRE

CYBER RÉSILIENCE

0.7

4.5 Les tests : le CHECK	
4.6 Boîte à outils techniques	
4.7 Le rôle d'une Direction de la Qualité	
Approche métier : Point de vue de Crisalyde	P.23
5. PENDANT LA CRISE	P.28
5.1 La détection	
5.2 Alerte	
5.3 Qualification	
5.4 Traitement	
Approche métier : Point de vue d'adista	P.31
6. APRÈS LA CRISE	P.36
6.1 RTO et WRT	
6.2 Le REX	
6.3 La limite des assurances cyber	
Approche métier : Point de vue de Gatewatcher	P.39
7. CONCLUSION	P.43
Approche métier : Point de vue de l'Agence du Numérique en Santé	P.44
8. LES 11 COMMANDEMENTS	P.48
9. ANNEXES	P.49
10. RESSOURCES	P.50

L'AUTEUR



Cédric CARTAU est RSSI et DPO du CHU de NANTES et du GHT44. Il est vice-président de l'APSSIS et enseigne à l'EHESP, à l'ESIEA et au CNEH. Il est également auteur de plusieurs ouvrages chez Eyrolles ou aux Presses de l'EHESP, sa dernière publication étant « La sécurité du système d'information des établissements de santé », en 2018.

cedric@cartau.net

L'auteur et l'APSSIS remercient ses contributeurs d'avoir accepté le difficile exercice de présenter une approche métier sur une question aussi complexe que la gestion de crise.



1. INTRODUCTION

Proverbe hébreu : « L'homme fait des projets et Dieu se marre »

Proverbe chinois : « Les tuiles des toits ont toutes été posées par temps sec »

Arriver au bureau un lundi matin...

Constater que son PC ne répond plus

Que le bureau des admissions est retourné au papier

Que l'identité des patients n'est plus transmise dans le système : transmissions de demandes d'examen en papier (3 fois plus lent), CR labo à la main, prescription et traça médoc à la main

Que les cuisines préparent les plateaux repas à l'aveugle

Que les transports patient doivent rappeler des brancardiers

Que la stérilisation est à l'arrêt

Que les blocs opératoires n'ont plus accès aux images, que la REA centralisée est HS et les personnels soignants doivent en urgence faire de la surveillance chambre par chambre

Que les appareils biomédicaux sont déconnectés du reste du système d'information : plus de supervision, plus de calibrage des appareils, plus de surveillance à distance des niveaux d'hélium ni des IRM par les fournisseurs

Que les Urgences et le SAMU sont retournés au papier

Que les plannings sont inaccessibles et que l'on ne peut plus prendre de RDV...ni voir les RDV passés

Que la saisie des actes est HS

Que la facturation au fil de l'eau n'est plus réalisée

Que les mandatements sont bloqués

Que les fournisseurs (qui ne sont plus payés) bloquent les commandes

et qu'en plus on n'a plus les coordonnées des fournisseurs pour les prévenir

... ni d'ailleurs la liste des codes produit à commander

Qu'il n'y a plus de gestion de stocks (médoc, réactifs labo, fournitures, etc.)

Que la messagerie ne fonctionne plus, à l'exception des (rares) fax encore en fonctionnement

Que par précaution, vos partenaires bloquent les échanges informatisés avec vous : EFS, CNAM, mutuelles, Ministère, ARS

Que la RH est bloquée

Qu'une partie des données (financières, RH, patients, GAM, DPI, labo, etc.) sera irrémédiablement perdue

Que le retour à la normale va prendre des mois...

... le tout sans accès Internet... voire sans téléphonie sur certains sites.

C'est une crise.

2. DÉFINITION DE LA CRISE

La seule question de la définition d'une crise fait débat, autant parmi les théoriciens du sujet que parmi les opérationnels (RSSI bien entendu, mais aussi les Urgentistes, les Décideurs, etc.).

En tant que définition académique, nous pourrions retenir ceci : « *Phénomène prenant naissance au sein des organisations, mis en éveil par un évènement déclencheur et dont la gravité peut être amplifiée par la présence de facteurs aggravants* ». Le Larousse précise quant à lui : « *Moment très difficile dans la vie de quelqu'un, d'un groupe, dans le déroulement d'une activité, etc. ; période, situation marquée par un trouble profond* ». En clair, ces définitions se basent sur le niveau de gravité de la situation, mais sans plus de précision.

Nous trouvons aussi des définitions dans les domaines économique, médical, psychiatrique, individuel, etc. Mais il apparaît rapidement deux notions importantes :

- La notion de gravité dans l'impact de la situation ;
- Le caractère paroxystique, qui distingue une crise de ce que l'on pourrait appeler « situation tendue ».

Par exemple, il est indéniable que l'apparition du COVID était une crise sanitaire mondiale, mais que la panne d'un datacenter dans un hôpital ne l'est pas forcément.

Une autre vision, plus opérationnelle, a tendance à retenir plutôt ce genre de définition : une crise, c'est quand il n'y a plus le manuel, plus de procédure expliquant comment faire.

Exemple

Crever un pneu n'est pas une crise : le manuel du véhicule vous explique comment changer la roue.

Mais crever un pneu, en pleine nuit et sous

une pluie battante, alors que vous étiez en train de conduire votre oncle en arrêt cardio-respiratoire aux Urgences, le tout en dehors de toute couverture GSM, voilà qui ne relève pas de la même qualification.

Dans l'aviation, considérant le triptyque « complexité, ressources, temps », on est en crise lorsqu'il n'existe plus de marge de manœuvre, c'est-à-dire une échappatoire sur l'un de ces paramètres.

Exemple

Dans l'exemple ci-dessus, concernant la première situation, s'il n'y a pas d'urgence, nous disposons d'une marge de manœuvre sur le facteur temps. En revanche, dans la seconde situation, nous n'avons ni le temps (situation médicale urgente), ni la possibilité d'appeler de l'aide (ressources additionnelles) ni de marge de manœuvre sur la complexité de la situation (on ne peut pas rouler sur la tranche du véhicule).

Point majeur : la crise est un phénomène au moins autant humain (de par la réaction des organisations et l'impact sur les processus) que technologique ou matériel. La désorganisation accroît l'ampleur de la crise, autant que l'impréparation.

Exemple

Le COVID19 était une crise. Mais si le COVID20 se déclare dans 5 ans ou 10 ans, cela ne devrait pas l'être, ou en tout cas l'impact sera mieux maîtrisé. A situation sanitaire égale, il est probable que le second ne sera pas une crise, en tout cas pas de la même ampleur.

Dans les faits, il y a bien entendu une notion de continuum : il n'existe pas de séparation claire et franche entre ce qui relève une situation de crise, ou pas.

3. LES FONDAMENTAUX

Pour dérouler les fondamentaux nécessaires au présent guide, nous prendrons comme hypothèse de travail que les Organisations ont un certain nombre de points communs avec le fonctionnement humain : dans une certaine mesure, la théorie des modes

mentaux s'appliquent aux Organisations, tout comme les concepts de sidération, de biais mentaux. La base théorique pourra être débattue, mais dans les faits ces analogies s'observent régulièrement sur le terrain.

3.1 Le concept de modes mentaux

Dans « Système 1 / Système 2 », Daniel Kahneman développe le concept des deux vitesses de la pensée. L'un des deux correspond aux réflexes (respirer, courir à la vue d'un prédateur, etc.) tandis que l'autre correspond à des actions apprises (conduire) et réfléchies.

Le domaine de l'aviation a une version presque identique et décrit trois modes mentaux :

- mode automatique, équivalent de la zone de réflexe (respirer) ou des actions que l'on fait sans réfléchir (débrayer en arrivant à un feu rouge, conduire sur le trajet de tous les jours pour rentrer du bureau, etc.) ;

Accidentologie

Une partie des accidents dans les transports provient du fait que la personne au volant était dans sa zone mentale automatique (celle qui FAIT les choses) alors que les circonstances extérieures (zone en travaux, rétrécissement de voies, etc.) auraient dû la faire passer à la zone réfléchie (celle qui PENSE les choses)

- mode réfléchi correspond à ce qui mobilise plus ou moins fortement notre attention : la phase d'apprentissage de la conduite, recevoir un coup de fil de son adolescent complètement perdu en centre-ville, etc. ;
- la zone de stress, qui est une extension du

mode réfléchi avec en plus l'inhabituel, le danger, l'urgence, etc.

Nous pourrions découper de façon plus fine en 4 ou 5 zones, mais au final, il faut retenir qu'il y a un continuum entre ces zones, et pas forcément de séparation marquée. Stricto sensu, une crise correspond à la zone de stress, ou plutôt à l'extrémité de cette zone de stress.

Entraînement aux pannes

Les pilotes d'avion professionnels doivent réaliser des entraînements en simulateur reproduisant des situations de panne de toute nature : panne d'un ou plusieurs réacteurs, feu à bord, etc. L'opérateur qui envoie les scénarii en temps réel au simulateur ajoute des pannes, des pannes aux pannes, etc. Tout le monde finit par craquer, tout le monde a une limite, mais l'entraînement permet de repousser cette limite et d'améliorer fondamentalement sa propre résistance - et celle de son Organisation - et ainsi d'étendre sa « zone réfléchie » et de repousser toujours plus loin l'extrémité de sa zone de stress.

3.2 Les facteurs humains

Par « Facteur humain », on entend toute action d'origine purement humaine et qui mène à l'incident ou à la catastrophe. Quand un pilote d'avion qui constate qu'un des deux réacteurs est en feu...arrête le mauvais réacteur¹ et que l'avion s'écrase (alors qu'un avion de ligne peut tout à fait voler avec un seul réacteur), l'accident est entièrement dû à un facteur humain.

Les erreurs absurdes

Dans cette sous-catégorie se classent les erreurs persistantes, c'est-à-dire pour lesquelles l'Organisation en cause a persisté

durablement. Christian MOREL a largement théorisé et creusé ce concept dans la suite « Les décisions absurdes », un classique du management, un indispensable à tout expert de la gestion de crise.

Dernièrement, un accident a été évité de justesse sur l'aéroport de Bordeaux², certainement dû à un enchaînement de causes humaines et évité justement grâce à la vigilance d'un pilote. Même les Organisations les plus résilientes ne sont pas à l'abri d'erreurs humaines.

3.2.1 Origine des accidents

Selon le BEA (Bureau d'Enquête et Analyse de l'aviation civile), 67 % des accidents ont une cause « Equipage » c'est-à-dire facteur humain. Les cas de panne simultanée des deux réacteurs existent mais sont rarissimes (moins de 5 par décennie dans l'aviation commerciale à mettre en regard des millions d'heures de vol), plus des 2/3 des accidents sont strictement imputables à l'erreur humaine.

Sans que cela ait une valeur statistique totalement fiable, selon mes fiches personnelles, plus de 50 % des incidents IT ont une origine « non-respect des processus de base », que ce soit par la MOA ou par la DSI. On apprend tout petit que l'on ne met

JAMAIS en production un vendredi, et on voit toujours des informaticiens (qui connaissent parfaitement cette règle) faire ce type de changement au motif que « oui mais là c'est urgent, pas de problème, j'ai bien testé ».

Les classiques

Compte admin créé pour une opération technique ponctuelle et jamais déprovisionné, règle Firewall ouverte pour une durée courte et jamais supprimée : les exemples sont nombreux où les DSI se mettent elles-mêmes dans une situation risquée, qui parfois conduit à une crise majeure.

3.2.2 Stress et performances

Il est avéré que l'individu moyen connaît une forte diminution des performances dans la zone de stress. Ce qu'il réalisera

sans difficulté en dehors de toute pression extérieure, il le fera avec le plus grand mal voire pas du tout quand le stress est à son

¹ « Les décisions absurdes », Christian MOREL

² <https://bea.aero/les-enquetes/evenements-notifies/detail/incident-grave-survenu-a-lairbus-a320-oe-ine-exploite-par-easyjet-et-au-robin-dr400-f-gtzy-le-31-12-22-a-bordeaux/>

maximum. Également, ces performances, déjà dégradées par une situation de stress, diminuent dans le temps lorsque la durée dans cette même zone de stress se prolonge.

La double peine

Non seulement dans une situation de crise, les performances de chaque individu ou de l'Organisation sont dégradées, mais en plus elles diminuent au fur et à mesure que le temps passe. Le facteur temps joue donc doublement contre nous.

On a vu, dans certaines situations de stress au long cours telles des remédiations à des

attaques cyber dans des grosses entreprises, des agents s'effondrer totalement avec crise de larmes à la clé et devoir être évacués de la zone de travail par la hiérarchie.

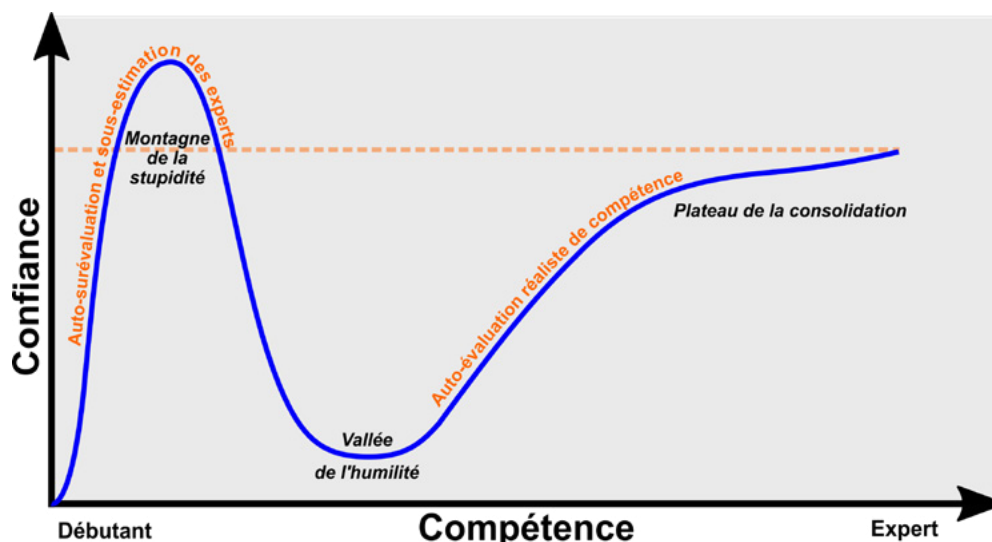
Réactions individuelles

Tel agent qui dans le quotidien est d'un calme olympien peut s'effondrer littéralement sous l'effet d'un stress intense ou long. Tel autre qui semble peu fiable a priori pourra au contraire afficher une résistance au stress hors du commun. Impossible de savoir comment réagiront les individus et cela ne doit pas engendrer de jugement personnel. On est comme on est.

3.2.3 Considérations additionnelles

L'effet de sidération est un phénomène à la fois individuel et collectif : il s'agit du temps d'immobilité qui suit directement un incident majeur. Les individus et les organisations ne savent comment réagir et les secondes et minutes perdues peuvent parfois être précieuses.

L'effet Dunning-Kruger est un grand classique dans la théorie des erreurs : il matérialise le fait que les « débutants » surestiment leur niveau de compétence, puis on assiste à un creux de perception au fur et à mesure que ces débutants acquièrent de l'expérience (et réalisent ce qu'ils ne connaissent pas) avant de voir la courbe repartir à la hausse avec l'expérience acquise. Il en va de même pour les Organisations nouvellement acquises à une technologie, un logiciel, etc.



https://fr.wikipedia.org/wiki/Fichier:Effet_Dunning-Kruger.png

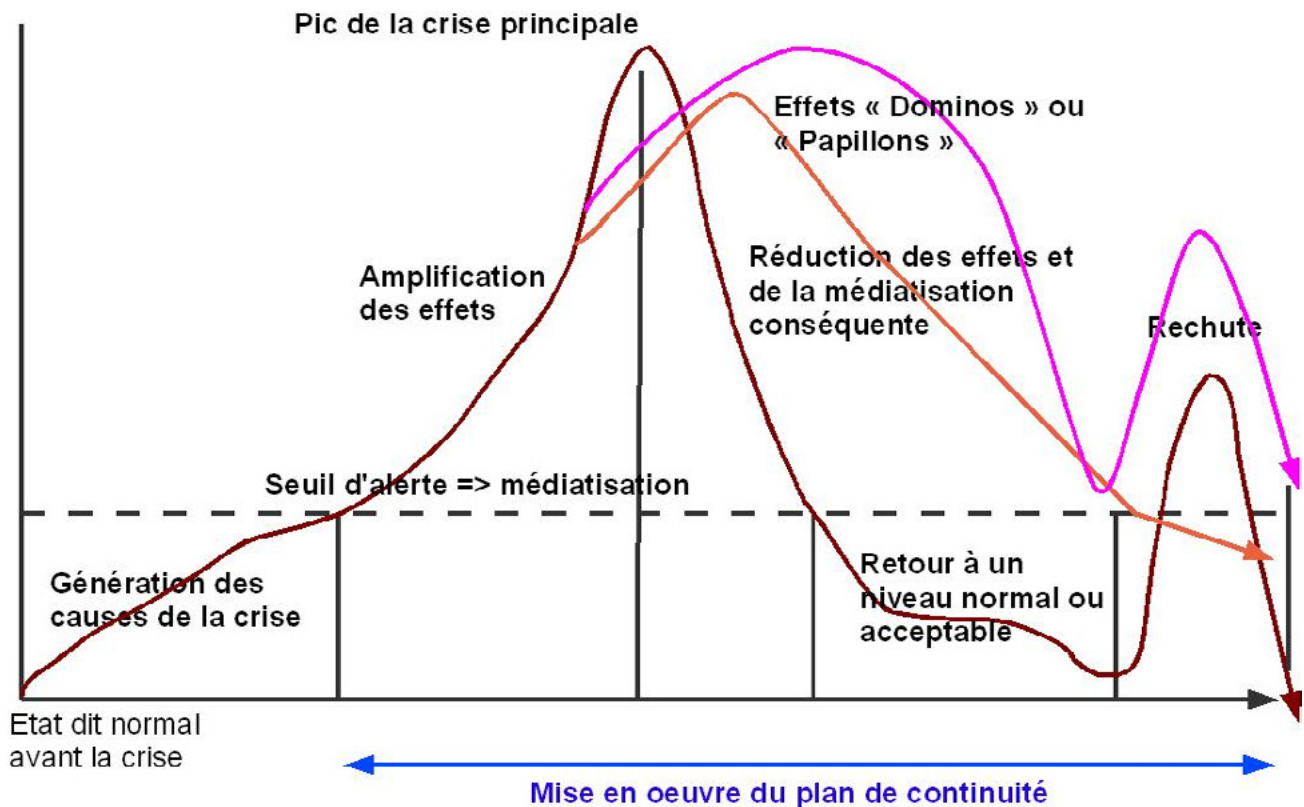
3.3 Les éléments d'une crise

Les origines d'une crise en général peuvent être multiples : catastrophe naturelle, catastrophe sanitaire, attaque terroriste ou cyber, etc. Une crise cyber peut être isolée ou au contraire consécutive à crise non-cyber : guerre de Crimée qui a eu, entre autres, pour

conséquence des attaques perpétrées par la Russie d'entreprises européennes évoluant dans cette partie géographique. Enfin il peut y avoir des impacts non-cyber de crise cyber : accident d'Epinal³ par exemple.

3.3.1 Points communs à toutes les classes de crise

La courbe en cloche de la crise est un grand classique, et décrit les grandes phases des réactions de l'Organisation face à une situation de crise. Ce genre de courbe est très courant, et se retrouve aussi dans les phases d'acceptation d'une nouveauté... ou tout simplement dans l'effet Dunning-Kruger évoqué plus haut.



³ <https://www.irsn.fr/savoir-comprendre/sante/laccident-radiotherapie-depinal>

Mauvaise nouvelle : la personne providentielle n'existe pas ou quasiment jamais : une crise n'est pas un film de *Marvel*. On sort d'une crise collectivement et avec la contribution de tous. Dans tous les cas, la réponse préventive à une situation de crise consiste en combinaison de dispositifs techniques et de dispositifs organisationnels: PCA/PRA/PSI, procédures dégradées, cellules de crise, etc.

Enfin, les grandes causes de déclenchement des crises cyber sont :

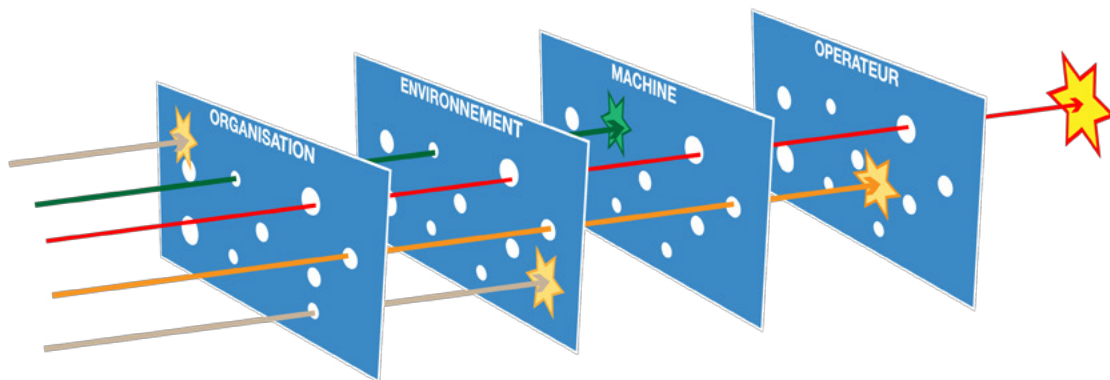
- l'erreur humaine : erreur directe, stupidité (naufage du Costa Concordia), non-respect des procédures, etc. ;
- l'erreur managériale, imputable à une personne, un groupe de personnes ou une

configuration organisationnelle ; l'explosion de la Navette Challenger peut se ranger dans cette catégorie ;

- l'accumulation d'Epsilon : il s'agit d'une somme de micro-erreurs ou dysfonctionnements qui, isolément, n'ont aucune conséquence, mais qui, mis ensemble, mènent à la catastrophe ; le naufrage du Titanic se classe dans cette catégorie ;

- la malveillance ;

- le dysfonctionnement des plaques de Reason : chaque dispositif de protection a bien fonctionné mais est par nature même imparfait, une erreur ou situation anormale a traversé toutes les couches de protection ;



3.3.2 Spécificités des crises cyber

Autre mauvaise nouvelle, qui est spécifique aux crises cyber pures : la cause n'est pas forcément visible. Il peut s'agir d'une intrusion silencieuse dans le SI avant déclenchement de charge virale. Cela peut durer des jours voire des semaines avant que la crise à proprement parler (ou plutôt ses effets visibles) se fassent sentir, la crise n'est pas forcément brutale et la situation peut dégénérer jusqu'à la crise. On ne voit pas ce genre de phénomène dans les autres secteurs subissant des crises.

Ransomware et signaux faibles

Bon nombre d'entreprises ayant subi des attaques en ransomware ont constaté, après coup, que les attaquants avaient un « pied dans la place » depuis des semaines et avaient mis à profit ce temps pour observer, cartographier, étudier le réseau avant de déclencher la charge virale.

En plus des généralités susnommées, une crise cyber :

- touche toute l'organisation, tous les processus et dure longtemps ; la crise cyber est d'ailleurs quasiment la seule à pouvoir bloquer toute une Organisation pendant des mois ou des semaines (en dehors de l'attaque nucléaire bien entendu, mais là on ne joue pas sur le même registre) ;
- touche le SLA / UC des fournisseurs (au sens processus) pour des services qui n'en ont pas conscience.

SLA et UC, les deux pièges d'une crise

Selon ITIL, tout processus comporte trois éléments macroscopiques :

- *le SLA (Service Level Agreement) : les services que le processus rend à des « clients » internes ou externes ;*
 - *l'OLA (Organisation Level Agreement) : l'organisation que le processus met en œuvre en interne (et qui peut être complexe ou multiple, une pharmacie de CHU comporte au moins 5 processus majeurs internes) ;*
 - *l'UC (Underpinning Contract) : il s'agit des contrats de service que le processus passe avec ses propres « fournisseurs » internes ou externes, l'UC du client est donc le SLA du fournisseur.*
- Les organisations humaines sont très*

accoutumées à la perte de leur SLA : les arrêts maladies, les démissions de personnels au mauvais moment, etc. En général les personnels présents compensent. Mais ces mêmes organisations n'imaginent pas qu'un de leur fournisseur majeur puisse lui-même être en défaut de SLA. Pour vous en convaincre, demandez à la DSI de couper la messagerie pendant 1 semaine et regardez la réaction des métiers au dysfonctionnement du SLA de la DSI qui est de facto une perte d'un de leurs outils de fonctionnement interne (UC).

- l'analyse des causes quelquefois longue et complexe;
- l'évolution peut être extrêmement rapide;
- une crise cyber ne relève pas forcément de la disponibilité : une fuite massive de données RH sur le Dark Web par exemple;
- dans la plupart des cas, une crise cyber relève tout de même de la disponibilité ou de la confidentialité ; le cas particulier des ransomwares touche à la fois de D (blocage du SI) et le C (exfiltration de données);
- les pires crises à gérer et à anticiper sont celles qui touchent l'intégrité des données, comme par exemple pour l'accident d'Epinal.

3.4 Les étapes de la gestion de crise

Une crise comporte trois temps :
Avant, il s'agit de la préparation.
Pendant, il s'agit de :

- la détection
- l'alerte
- la qualification
- le traitement

Après, il s'agit de la capitalisation.

3.5 Aux confins de la crise

Les professionnels de la gestion de risques le savent, la faute impardonnable n'est pas de subir une crise, mais:

- soit de subir une crise de la même ampleur que la précédente à cause identique et à impact identique ; cela veut dire qu'il n'y a eu aucune capitalisation lors de la crise précédente ;

Deux exemples de crises qui ne doivent pas se reproduire

Le COVID et la crue majeure de la Seine à Paris. Car elles se sont déjà produites.

- soit de subir une crise dont les causes étaient évidentes et les impacts faciles à anticiper. Dans ce cas, les experts parlent de « zone d'humiliation ».

Un exemple évident

Ne pas avoir prévu de sauvegardes face à une attaque de ransomware.

Il existe au moins 4 limites et les experts doivent « faire leur deuil » de leur limite d'action :

- l'impondérable, c'est-à-dire la crise qui ne s'est jamais produite.
- les crises de classe Black Swan, dont les probabilités d'occurrence sont extrêmement faibles mais l'impact quasi infini ; le Tsunami d'Asie en 2004 par exemple, ou l'éruption du Vésuve en 79 après Jésus Christ, qui a totalement détruit Pompéi.
- la limite de la mémoire humaine ; on peut citer les inondations de Vaison La Romaine en 1992 ; après-coup des historiens sont allés fouiller dans les archives de la ville et ont découvert qu'un événement d'une ampleur

équivalente se produisait tous les siècles, mais que l'on en avait perdu le souvenir.

- enfin, la limite des moyens ; quels que soit les dispositifs de prévention (techniques ou organisationnels), il existe toujours une limite (plaques de Reason) à ce que l'on peut prévoir et à ce à quoi on pourra faire face.

Darwin et crises

Les civilisations qui ont connu des crises majeures et qui en parlent dans leur folklore et mythes communs sont justes celles qui ont survécu. Les autres ne sont plus là pour en parler : les Etrusques, les Mayas, etc. Et justement la cause de leur disparition est souvent inconnue ou imprécise.

Le seul objectif d'un expert en gestion de crise est de ne pas devenir la civilisation Maya de la cyber, sur laquelle les archéologues du futur se pencheront en se demandant ce qui a bien pu se produire qui a enseveli telle Organisation, telle Civilisation, etc.

LE SECTEUR DE LA SANTÉ EN FRANCE FAIT FACE À DE NOMBREUX DÉFIS EN MATIÈRE DE CYBERSÉCURITÉ

Par Christophe Badot, Directeur Général France, CrowdStrike

Approche métier : Point de vue de CrowdStrike

Les DSI et les RSSI dans le secteur de la santé sont aujourd'hui confrontés à de très nombreuses difficultés. Les hôpitaux cherchent donc de nouveaux moyens pour financer leurs besoins technologiques et mettre en place des mesures en matière de cybersécurité afin de rester opérationnel et de maintenir la qualité des soins. Parmi ces défis, nous retrouvons :

1. L'augmentation des coûts : Les hôpitaux sont susceptibles d'être confrontés à la pression continue de l'augmentation des coûts de main-d'œuvre, d'approvisionnement et ceux liés aux investissements technologiques du secteur.

2. Les enjeux liés aux fusions et acquisitions : Lors de l'intégration des systèmes informatiques dans le cadre d'une fusion-acquisition, il existe des failles potentielles qu'un adversaire peut exploiter lors des changements structurels de la pile technologique d'une organisation. Au cours du processus de fusion et d'acquisition dans le secteur de la santé, il est courant que les organisations se concentrent sur l'intégration des finances et de la technologie. Cependant, il existe souvent un

angle mort crucial lorsqu'il s'agit de sécuriser les données de santé impliquées tout au long de la transaction, et les acteurs de la menace considèrent souvent ces transactions comme des vulnérabilités exploitables.

3. La pénurie de main-d'œuvre : La pénurie de main-d'œuvre dans le secteur de la santé peut entraîner une augmentation des coûts associés, les hôpitaux se faisant concurrence pour recruter du personnel qualifié. Il peut en résulter un recours accru aux agences de recrutement temporaire et au paiement d'heures supplémentaires pour le personnel en place.

4. Les risques liés à la cybersécurité : Avec l'apparition du COVID-19, le secteur a dû effectuer un changement rapide en matière de technologie pour permettre aux patients de bénéficier de la télémédecine et aux professionnels de la santé de travailler à distance. Après la pandémie, ces tendances se maintiennent, laissant le secteur de la santé exposé à un autre vecteur d'attaque. En 2023, [le volume des intrusions interactives a augmenté de plus de 60 % d'une année sur l'autre](#), le secteur de la santé figurant parmi les dix premiers secteurs ciblés. Les informations personnelles identifiables (PII)

stockées par les hôpitaux sont une ressource critique que les adversaires cherchent à exploiter.

Une situation d'urgence en matière de cybersécurité

L'augmentation des coûts et la pénurie de main-d'œuvre obligent les organismes de santé à faire plus avec moins. Avec la menace croissante des brèches de données, il y a peu de place pour l'échec.

Aujourd'hui plus que jamais, les décideurs du secteur de la santé considèrent qu'une faiblesse en matière de cybersécurité constitue un risque critique pour l'entreprise - un risque qui doit être traité en priorité par le conseil d'administration et les équipes de sécurité. Les stratégies de sécurité sont

désormais largement intégrées dans les programmes existants de gestion des risques et de gouvernance des hôpitaux, en tant que pierre angulaire du cadre de continuité des activités. En effet, un programme de cybersécurité solide atténue efficacement les risques. Les organisations sont ainsi en mesure de prévenir les impacts négatifs sur les résultats cliniques, minimiser les coûts et les perturbations et préserver des soins de haute qualité.

Les outils pour répondre à ces enjeux : CrowdStrike Falcon®

La plateforme CrowdStrike Falcon® offre une rentabilité immédiate tout en éliminant la complexité et en simplifiant le déploiement pour réduire les coûts opérationnels. CrowdStrike Falcon® Cloud Security protège les organisations tout en préservant la charge de travail et les effectifs partout et à tout moment.

La cybersécurité ne se limite pas à la technologie - elle nécessite également une expertise permanente et des processus rapides à mettre en place. CrowdStrike Falcon® Complete managed detection and response (MDR) apporte une expertise ciblée pour stopper les menaces grâce à

une vigilance continue et met à disposition des chasseurs de menaces reconnus qui tirent parti de la puissance de la plateforme CrowdStrike Falcon®. Falcon Complete MDR permet à CrowdStrike de devenir, aux yeux de ses partenaires, une extension de leur propre équipe de sécurité. Falcon Complete agit sur les terminaux, le cloud ainsi que sur le vol d'identité, cherchant à résoudre en amont les failles et permettre aux clients de se prémunir face aux futures menaces.

Le rôle du secteur de la santé dans l'amélioration des programmes de cybersécurité

Les organismes de santé doivent rechercher des technologies qui offrent une rentabilité immédiate tout en simplifiant le déploiement et en éliminant la complexité au sein de l'environnement afin de réduire les coûts opérationnels. Les organisations ont besoin de technologies défensives basées sur le cloud comme [la plateforme CrowdStrike Falcon® XDR](#) qui sécurise les workloads et les effectifs n'importe où, n'importe quand, sans compromettre la vitesse ni la performance. Avec la bonne combinaison de personnes, de processus et de technologies, les prestataires de soins de santé peuvent éliminer les menaces sur les terminaux, les workloads dans le cloud et assurer la protection des identités, ce qui aide à résoudre complètement les problèmes et permet aux organisations de garder une longueur d'avance sur les menaces tout en

garantissant des soins optimaux aux patients. CrowdStrike a pour mission de mettre fin aux brèches pour permettre au secteur de la santé de continuer à innover et à sauver des vies. Grâce à sa plateforme, sa technologie et son expertise, CrowdStrike permet à ses clients de garder une longueur d'avance sur l'adversaire. Dans cette optique, sont réunies les protections essentielles telles que la détection et la réponse étendues aux terminaux, la protection contre les menaces liées à l'identité, la sécurité du cloud, la gestion des vulnérabilités et des risques, la threat intelligence et bien plus encore - le tout sur une seule et même plateforme. Pour en savoir plus sur la façon dont CrowdStrike peut aider les organismes de santé, visitez notre site Web : <https://www.crowdstrike.com/solutions/healthcare/>



www.crowdstrike.com

4. AVANT LA CRISE : LA PRÉPARATION

4.1 Visions globales

Il existe plusieurs visions de la période de préparation. Aucune n'est vraie plus que les autres. Elles sont juste complémentaires.

4.1.1 La vision darwinienne

Elle consiste à voir les crises comme un processus de sélection darwinien des Organisations, tel qu'évoqué plus haut dans l'encart sur les Etrusques et les Mayas.

Il faut notamment prendre garde au biais du survivant : si une Organisation a résisté à une crise majeure avec tel ou tel dispositif global, ce n'est pas forcément la preuve de l'efficacité dudit dispositif. Peut-être que

nombre d'Organisations similaires avaient utilisé le même dispositif mais ne sont plus là pour en parler car elles ont disparu.

Enfin il faut aussi tenir compte de la limite du concept de mort d'une Organisation : cela peut avoir du sens pour une entreprise privée, mais difficilement pour une grande administration ou un Etat.

4.1.2 La vision risques

Cela consiste à vouloir faire passer les risques cyber de la classe « danger » à la classe « risque ».

De la différence entre un danger et un risque

La voltige aérienne est une activité risquée, mais pas dangereuse : on dispose de statistiques, d'une antériorité sur les pannes, de dispositifs testés et éprouvés de réduction des risques, etc.

A contrario, le vol Wingsuit est une activité dangereuse : peu de contre-mesures aux risques.

Le risque est assurable, le danger ne l'est pas.

Un risque est quantifiable (probabilité et impact), un danger ne l'est pas.

Cela consiste donc à réaliser une appréciation des risques, à les quantifier, à mettre en place des dispositifs de réduction, à quantifier les risques résiduels, etc. On parle EBIOS, MEHARI, etc.

Cette approche conduit, poussée à l'extrême, à publier un catalogue des risques identifiés avec pour chacun le risque résiduel accepté. Ce qui est dans le tableau a fait l'objet d'un passage de la classe des dangers à la classe des risques (sauf mention contraire dument acceptée par la MOA), ce qui n'est pas dans le tableau n'est pas pris en compte.

4.1.3 La vision mode mental

Si l'on reprend les propos génériques des premiers chapitres du présent ouvrage,

cela revient à inoculer de la résilience aux MOA et étendre leur zone réfléchie et ainsi

repousser la limite avec la zone de stress. De la même manière que les pilotes de ligne s'entraînent aux pannes en vol pour être en zone réfléchie quand la panne surviendra.

4.1.4 Vision Deming

Enfin la vision Qualité consiste à faire rentrer tout le dispositif de gestion de crise dans un cycle général PDCA, ce qui implique :

- De construire un dispositif technique et organisationnel (PLAN) et de le mettre en œuvre (DO) ;
- De ne surtout pas chercher l'exhaustivité mais de le tester (CHECK) ;

- De systématiquement améliorer le dispositif, soit en retour des tests, soit à la suite d'un incident.

Dans cette dernière approche, l'amélioration continue prime largement sur l'exhaustivité d'un dispositif qui risque d'être immobile, donc rapidement inutile.

4.2 Se préparer : le BUILD du PDCA

Il faut bien distinguer 2 notions :

- la préparation d'un dispositif de crise est un projet en soi ; au sens SI, il s'agit donc d'un BUILD ;
- le livrable de ce projet est un dispositif qui est de facto une roue de Deming, ou dit autrement un dispositif PDCA qui va ensuite devoir fonctionner ; au sens SI, il s'agit d'un RUN.

En d'autres termes, il s'agit de réaliser le BUILD d'un PDCA, PDCA qui passera ensuite en mode RUN. Ce dispositif PDCA comporte l'ensemble des éléments de préparation à la crise (PLAN), va servir pendant une crise (DO), et doit donc être testé (CHECK) et amélioré (ACT).

Corolaire de ce découpage, la gouvernance du dispositif de BUILD n'est pas forcément la même que la gouvernance du PDCA : le chef de projet qui va « BUILD » tout le dispositif de cellule de crise n'est pas forcément la même personne qui va assurer que la roue PDCA fonctionne.

Pour la phase PLAN, un sponsoring de haut niveau est indispensable : il doit d'agir de la Direction Générale, sans laquelle le Chef de Projet va s'épuiser pendant des mois sans résultats. Des leviers organisationnels tel le rajout dans les objectifs de pôle des tests de cellule de crise vont faciliter le travail de ce chef de projet. Les candidats à la chefferie de ce type de projets sont multiples : informaticien avec le volet applicatif, médecin, qualitatif, RSSI, etc.

« Quand la crise arrivera, vous prierez que vos précédents CHECK auront été efficaces, car vous n'aurez que le DO sur lequel compter »

4.3 Spécificités du PLAN dans la santé

Sans surprise, les directions concernées à la fois par le BUILD et le RUN sont : la Direction Générale, la CME, la Direction des Soins, la Direction Juridique, la Direction de la Communication, la Direction des Usagers, bien entendu la DSI, et l'ensemble des MOA concernées par la criticité du SI (autant dire toutes).

S'il est nécessaire de séquencer le projet du fait de son ampleur, il faudra adresser en priorité :

- les fonctions support au soin : laboratoire, imagerie et pharmacie ;
- les fonctions support logistique : approvisionnements / commandes (médicaments, etc.), transports patients, restauration, etc. ;
- la téléphonie ;
- la cellule de gestion de crise de niveau DG, afin de lui adjoindre les spécificités d'une crise cyber ;
- et bien entendu la DSI qui sera systématiquement concernée.

4.4 Les livrables du BUILD

Lorsque le BUILD sera terminé, l'établissement disposera des livrables suivants, découpés selon la vision PDCA qui reste de loin la meilleure approche.

4.4.1 Gouvernance globale

PLAN :

- Un document chapeau de politique générale de la gouvernance des crises cyber mentionnant des objectifs macro (couvrir x % de l'établissement, garantir la sécurité des patients, etc.).

DO :

- Un descriptif de l'organisation générale comprenant, entre autres, l'articulation entre le dispositif de crise cyber et le dispositif de crise générale, une procédure de communication ;
- Un document de fonctionnement opérationnel de la cellule de crise niveau Direction Générale : canaux de

communication, lieux de rassemblement, ouverture des portes sécurisées en heures non ouvrables, etc. ;

CHECK :

- Un plan de test (CHECK) de tout le dispositif ;
- Une consolidation des plannings de test de cellule de crise de chaque MOA à des fins de pilotage global ;

ACT :

- Un suivi des actions.

4.4.2 Dispositions par MOA

PLAN :

- Un document tactique de crise cyber pour chaque MOA mentionnant des objectifs macro (labo : pouvoir délivrer x % des analyses pendant 3 mois ; pharmacie : pouvoir approvisionner en médicaments les urgences et la réa, etc.). Ces éléments sont absolument majeurs et doivent être remontés au niveau stratégique pour assurer un pilotage global d'une crise cyber au niveau de tout l'établissement.

DO :

- Le dispositif organisationnel en cas de crise ;

- Autant de procédures ou mode opératoire que nécessaire selon les outils utilisés au quotidien (que faire en cas de panne de tel ou tel outil logiciel).

CHECK :

- Un plan de test de cellule de crise.

ACT :

- Un suivi des actions de correction.

4.5 Les tests : le CHECK

Les tests sont un sujet en soit. Les typologies de tests sont :

- les tests techniques versus les tests organisationnels ;
- les niveaux des tests : débutant / intermédiaire / avancé, selon une typologie à déterminer ;
- les tests globaux (tout l'établissement) ou par processus métier ;
- les tests avec ou sans perturbation ;
- cas particuliers, les tests peuvent être restreints ou pas aux canaux de communication et à la connaissance des procédures ; c'est la version la moins intrusive des tests et c'est le « minimum syndical ».

Il n'existe pas de méthode parfaite en la matière : certains commencent par des tests techniques (redondance des

infrastructures) et engagent ensuite des tests organisationnels. Certains démarrent par des tests « légers » (test des canaux de communication et des procédures à jour) et engagent ensuite des tests organisationnels. Il existe tout de même des règles à observer, et notamment :

- ne pas se contenter d'une seule typologie de tests, il est indispensable de varier ;
- a minima, les canaux de communication doivent être testés régulièrement : existence d'annuaires à jour de contact des personnels du service ou de la cellule de crise (liste à jour, accessible facilement, existence de listes de diffusion sur Signal / Tchap ou autre messagerie instantanée sécurisée, etc.) ;
- privilégier la fréquence sur l'exhaustivité des tests : il vaut mieux un test par trimestre et par MOA sur des périmètres

très restreints, qu'un test unique tous les 3 ans ;

« En matière de tests de cellule de crise, small is beautiful »

- la gouvernance de tout le dispositif de gestion de crise cyber doit disposer d'un pilotage global de l'ensemble des tests à l'échelon de l'établissement, avec un registre des contrôles (procédures formalisées) et un calendrier a minima annuel, ce qui permet d'ailleurs de disposer facilement d'indicateurs. Ce point est absolument majeur.

4.6 Boite à outils techniques

Rapidement apparaît la nécessité d'une boite à outils techniques cyber. Chacun pourra se constituer ses propres listes, mais à minima elle doit comporter :

- des canaux techniques alternatifs de communication : dans toutes les crises cyber, en l'absence de messagerie électronique (et parfois de téléphonie si elle est sous IP), les personnels ne peuvent plus communiquer entre eux ; le choix institutionnel d'outils de messagerie alternatifs (Signal et Tchap sont les principaux) est indispensable, avec la création des groupes et listes de diffusion adéquats (testés, à jour et révisés) ;
- des outils techniques d'analyse on-line de malware : [virustotal.com](https://www.virustotal.com) est le plus connu, mais il y a aussi des équivalents quasiment chez tous les éditeurs dans ce domaine ;
- une bibliothèque d'outils d'analyse variés : PingCastle, BloodHound, analyseurs réseau, etc. ;
- une définition interne officielle de classification des documents (protocole TLP⁴)

Le kit de survie

<https://www.pingcastle.com/>

www.nmap.org

www.virustotal.com

<https://www.urlvoid.com/>

⁴ <https://www.cert.ssi.gouv.fr/csirt/politique-partage/>

4.7 Le rôle d'une Direction de la Qualité

Il est clair, au regard des éléments ci-dessus, que l'ensemble de tout le dispositif s'inscrit parfaitement dans une démarche qualité :

- les éléments de stratégie, que ce soit au niveau global établissement que par MOA, relèvent d'un PLAN ;
- les livrables relèvent du DO ;
- les éléments des tests (périmètre, calendrier, suivi) relèvent du CHECK ;
- le suivi des actions relève du ACT.

On retrouve d'ailleurs tout l'intérêt d'une démarche ISO, à savoir :

- la séparation du fond et de la forme ;
- le pilotage par les processus et les indicateurs ;
- la formalisation d'objectifs stratégiques niveau DG avec des revues a minima annuelles remontant les indicateurs collectés.

Pour toutes ces raisons, le pilotage par un qualicien de tout ce dispositif est envisageable, autant que par un RSSI qui ait un profil métier plutôt que technique pur. Que l'on parte d'une 9001 ou d'une 27001, on finit par retrouver ses petits, avec un avantage concurrentiel de la 27001 qui a pour elle les concepts de contrôles et de DDA.

« Si le DO est l'arme des MOA pendant la crise, le PDCA est celle du gestionnaire du dispositif global de crise cyber. »

COMPRENDRE LES EFFETS D'UNE CYBERATTAQUE : LA RÈGLE DE 3

Par les équipes de Crisalyde

Approche métier : Point de vue de Crisalyde

Se préparer à affronter une crise, c'est en premier lieu la comprendre. Il s'agit du premier pas à passer pour appréhender des crises cyber très particulières à 2 égards : leur aspect endogène d'une part ; et leur temporalité d'autre part.

Endogène car, depuis des décennies, le système de santé se prépare aux crises sous un angle précis : être en capacité d'accueillir plus de patients. Ici, la crise est toute inverse : le flux de patient reste inchangé, mais l'établissement perd ses capacités intrinsèques qui permettent la prise en charge.

Mais nous allons ici surtout nous concentrer sur la temporalité. Car une cyberattaque se

caractérise par une cinétique très particulière en 2 temps : une première phase courte de très haute intensité, suivie d'un temps long où la crise finit par se mêler au quotidien dans un effet parasite réciproque.

Au gré des expériences de crises des équipes de Crisalyde, nous avons théorisé un modèle empirique permettant de mieux saisir ces aspects : *"la règle de 3"*. Chaque cyberattaque étant spécifique, il ne faut pas prendre les temporalités présentées avec une précision horlogère, mais utiliser ce modèle pour comprendre les différentes phases et enjeux auxquels un établissement pourrait être confronté.

3 heures : la sidération

« Une crise mal démarrée est une crise mal gérée » : adage que nous répétons à loisir à qui veut bien l'entendre.

Une cyberattaque mal qualifiée, ou trop tardivement, peut changer drastiquement la donne. Nous l'avons bien vu ces derniers mois à l'occasion d'attaques détectées et stoppées à temps : une heure de gagnée dans la réaction, peut potentiellement réduire d'un mois le retour à la normale.

Car lorsque l'attaque a commencé, c'est une course contre la montre qui se lance, avec 2 objectifs prioritaires : la protection

des patients, et la protection du système d'information (ultimement, au bénéfice du patient).

Dans ces 3 heures, l'attaque doit être détectée, et l'établissement s'organiser pour :

- Décider rapidement d'actions d'endiguement, et notamment d'isolation du SI d'internet, voire de tout le réseau local. Sachant qu'à ce stade, une telle décision aura à court terme des conséquences bien plus déstabilisantes que celles

actuellement provoquées par l'attaque. Métaphoriquement : décider d'amputer la jambe parce que l'orteil est gangrené, parce que l'on sait que l'infection est potentiellement en train de remonter sans être visible...

- ... Tout en donnant la possibilité (et le temps) de prévenir les personnels, transmettre des conduites à tenir, et peut-être s'offrir le luxe de 30 minutes pour imprimer les dossiers patients et entrer de manière plus sereine en mode dégradé à l'échelle de l'établissement tout entier.
- Mobiliser la cellule de crise et les équipes informatiques, et réussir à trouver un mode de fonctionnement qui permette à la DSI de donner les informations attendues - du

point de vue métier - permettant la prise de décision.

- Potentiellement décider de procéder à une déprogrammation et / ou au rappel de personnel.
- Contacter l'ARS et le SAMU pour organiser un délestage, le CERT-Santé pour mobiliser les expertise cyber.
- Sans oublier de mettre en sécurité les sauvegardes, qui seront décisives un peu plus tard.

Une liste d'actions fournie, à réaliser malgré la sidération, l'incertitude complète, et potentiellement à 2 heures du matin dans la nuit de samedi à dimanche.

3 jours : l'expiration des modes dégradés

Deux dynamiques très différentes vont s'installer dans l'établissement au cours des 3 premiers jours.

Dans les services règne un calme relatif. L'activité est réduite du fait des délestages et déprogrammations ; le personnel est pleinement dédié aux soins sans tâches administratives informatiques ; les modes dégradés permettent de garantir la continuité et la sécurité des soins. La situation est à peu près la même sur le plateau médico-technique et dans les services administratifs. En revanche, la cellule de crise et la DSI bouillonnent (chacune à son rythme et sur ses propres enjeux), et subissent toujours une grande incertitude : il faudra plusieurs jours pour comprendre l'ampleur de l'attaque, identifier le vecteur d'intrusion, récupérer la main sur une partie du SI, savoir ce que

l'on peut utiliser et ce qui doit rester sous scellé... Ces 3 jours suffisent à peine à faire venir les renforts spécialisés et leur donner les accès pour commencer à travailler. Tandis que l'impact sur l'offre de soin territoriale devient pesant.

Et, le troisième jour, tout bascule. Car, dans la très grande majorité des cas, les modes dégradés dans les hôpitaux présentent 3 caractéristiques : ils concernent un scénario de panne isolée ; ils sont prévus pour fonctionner 2 ou 3 jours ; et ils concernent les activités de soins, pas les fonctions supports.

Prenez votre procédure dégradée d'admission : un dispositif parfaitement rôdé qui consiste en un stock de 1000 plaquettes d'étiquettes, avec des IPP dédiés, et un remplissage à la main de l'identité du

patient. Parfait pour faire face à une panne du logiciel de GAM.

Sauf que vous traitez un flux moyen de 300 patients par jour : vous voyez où mène le calcul.

Par ailleurs durant ces 3 jours, la pharmacie s'est totalement réorganisée pour délivrer les médicaments à la main et répondre aux besoins des services. Mais voilà : elle n'a plus aucune vision sur son inventaire, en plus d'avoir perdu tous ses moyens de passer des commandes.

Ainsi, la difficulté majeure d'un service ne réside souvent pas dans ses propres

dysfonctionnements : mais le fait qu'il ne puisse pas s'appuyer sur tous les autres maillons de l'hôpital.

Ajoutez à cela des pannes informatiques à rebours causées par les isolations réseaux, comme par exemple les baux DHCP du matériel biomédical qui expirent, puisque le serveur DHCP n'est plus joignable.

Il est donc essentiel, dans ces 3 premiers jours, de faire comprendre à toute l'organisation que la situation va durer, que ces incertitudes vont demeurer plusieurs jours, et qu'il faut très rapidement anticiper la manière de pérenniser les modes dégradés.

3 semaines : le mode dégradé pérenne

Il faudra environ 3 semaines pour lever les incertitudes. Mener à bien les investigations, comprendre la compromission, exclure toute menace rémanente, retrouver des accès à l'administration du système.

Durant ces 3 semaines, la situation informatique restera au mieux "frugale". Il est impossible de redonner un ordinateur, une connexion internet, une adresse courriel à chaque agent. Et encore moins l'utilisation des logiciels métiers et la multitude d'interconnexions qu'ils comportent.

Imaginez la situation du DSI qui, fièrement, a pu se faire livrer 150 ordinateurs et 50 clés 4G dans un délai record, et qui se retrouve livré à 2500 utilisateurs qui ont tous besoin "de toute urgence" de matériel. Et les 150 heureux élus de revenir le lendemain en disant que sans tel ou tel logiciel, en fait ils ne peuvent rien faire de leur ordinateur.

Comment identifier, mesurer et objectiver les services où il faut mettre en priorité le peu d'informatique que l'on peut mettre

à disposition ? Comment organiser ce déploiement, les explications aux utilisateurs de ce qu'ils peuvent ou ne peuvent pas faire, en s'assurant de ne pas créer une nouvelle brèche de sécurité ? Sans anticipation et planification (voir l'encadré sur le PCA), le traitement de cette problématique s'avère rapidement kafkaïenne.

La conduite à tenir de l'établissement durant ces 3 semaines est un exercice d'équilibriste permanent : assurer l'avancée des investigations informatiques ; surmonter les limites des modes dégradés pour mettre en œuvre des modes dégradés pérennes ; reprendre des activités de soins qui ne peuvent plus tolérer de retard ou de déprogrammation ; informer régulièrement le personnel, sans moyens de communication ; informer et rassurer les patients et familles...

Événement bonus : c'est à ce moment-là que les hackers divulguent sur le dark web les données volées sur le SI de l'hôpital.

3 mois : retour à la normale... ou création d'une nouvelle normalité

Au terme des 3 semaines d'investigation, l'information la plus importante de cette crise arrivera finalement : est-il possible de redémarrer le système... ou faut-il le reconstruire ? Trois grands cas de figure se présentent :

1. L'attaque a été contenue, le système est globalement sain, il est prêt à repartir après quelques réparations et un peu de sécurisation. On a vu ce scénario se dérouler ces derniers mois sur des attaques traitées de manière précoce.

2. L'attaque a fait d'importants dégâts, mais les sauvegardes sont saines et le SI

est globalement à l'état de l'art. Il va être possible de redémarrer le système, en suivant des procédures de dépollution et de sécurisation strictes, et progressivement redonner des services aux utilisateurs. Comptez environ 3 mois pour traiter 80% des applications. Question : dans quel ordre les traitez-vous ? Quelles en sont les interdépendances ?

3. L'attaque a fait d'importants dégâts, les sauvegardes ne sont pas exploitables et/ou le système est trop obsolète pour être redémarré en l'état. Dans ce scénario, la règle de 3 reste applicable : il faudra 3 ans pour reconstruire pleinement le SI de l'hôpital...

Le Plan des plans

La préparation aux crises s'appuie beaucoup sur des plans, et il peut être aisé de se perdre dans la liste. Voici un memento rapide pour naviguer avec aisance dans le sujet :

• **Plan "Situations sanitaires exceptionnelles"** : outil de la cellule de crise hospitalière qui permet notamment de mettre en place l'organisation de crise, et l'accompagner dans les prises de **décisions stratégiques** et les actions systémiques à mettre en œuvre. La pratique démontre qu'un volet "Numérique" (accident ou cyberattaque) de ce plan a tout son intérêt pour faire face à ces scénarios, tout en conservant cette approche de document unique de référence du pilotage de crise de

l'établissement. Ce plan est essentiellement utile pour faire face aux 3 heures et 3 jours.

• **Plan de Continuité et Reprise d'Activité (PCRA)** : un inventaire des activités métiers prioritaires (soins et fonctions supports), réparties par temporalité, avec des solutions anticipées pour faire face à un scénario de disruption. C'est grâce à ce plan que les personnels sauront comment travailler sans ordinateurs, que la DSI saura à qui distribuer quels ordinateurs de secours quand, etc. Le PCRA est le document qui permet de couvrir les phases 3 jours, 3 semaines et 3 mois en réduisant au maximum l'improvisation. Il anticipe également les besoins liés au retour à la normale, par exemple pour réintégrer

dans l'informatique tout ce qui a été fait en mode papier.

- **Plan de Reprise Informatique (PRI)**, parfois également appelé Plan de Reprise d'Activité (PRA) ou Plan de Secours Informatique (PSI) : sur la base des priorités métiers identifiées dans le PCRA, le PRI est un document décrivant comment reconstruire le système d'information de l'établissement. Dans quel ordre procéder, comment prendre en compte les interdépendances applicatives, quelles compétences internes et externes mobiliser... C'est la recette de qui permet de "cuisiner" le SI reconstruit.

- **Modes dégradés / procédures opérationnelles** : au plus proche des personnels, une description très précise et détaillée permettant de mettre en œuvre

les stratégies identifiées dans le PCRA. Par exemple : le PCRA identifie la paie comme une activité critique ; la solution de continuité identifiée est de demander au Trésor Public l'exécution de la paie du mois N-1 à l'identique ; la procédure opérationnelle comporte le numéro de contact, les informations d'identification à communiquer, la chaîne de validation requise, etc.

Et n'oubliez pas, un plan ne vous sera pas utile s'il est stocké sur un dossier réseau chiffré par le pirate : tous ces documents indispensables (et bien d'autres encore, comme des dossiers patients vierges et prêts à imprimer) ont tout intérêt à être stockés sur un support que vous tiendrez scrupuleusement éloigné de tout port USB ou réseau !



<https://crisalyde.fr/>

5. PENDANT LA CRISE

Décrire le dispositif pendant la crise est un exercice qui atteint vite ses limites, puisque par définition la crise relève de l'impondérable et de l'imprévisible. Si l'organisation survit à la crise (qui est un

CHECK grandeur nature), elle mettra à jour ses dispositifs et ses procédures (ACT) jusqu'à la prochaine crise.

Il existe tout de même des points d'attention à garder en tête.

5.1 La détection

Le problème majeur est la détection des signaux d'une crise qui, dans le cas d'une crise cyber, sont souvent des signaux faibles : un PC infecté, un compte admin nouvellement créé dans l'AD, voire une CPU surchargée sur un serveur en DMZ. Il n'existe aucune solution connue pour cette détection de signal faible, et les vendeurs de produits type EDR font des promesses qui n'engagent que ceux qui y croient.

D'autant que se pose la question de sur-réagir ou pas. Si au moindre doute, on coupe Internet ou une partie de l'infrastructure, ça risque rapidement de tourner au syndrome du conte de Pierre et le Loup : plus personne ne va finir par vous croire, y compris quand l'alerte sera réelle et sérieuse.

Le temps d'analyse est majeur en cas de signal fort ou faible, en se méfiant comme de la peste du biais de confirmation, ce biais

cognitif qui a tendance à nous faire voir ce que l'on croit voir et pas l'inverse.

« Détecter, détecter, et ne pas oublier que l'absence de preuve n'est pas la preuve de l'absence. »

L'entraînement aux exercices et la paranoïa cyber semblent être la seule solution, ce qui finit en revanche par mettre à rude épreuve les nerfs et les organismes des experts cyber - et si on a un tel turn over dans ce métier, ce n'est peut-être pas pour rien. Avec le risque de tomber dans le syndrome Hoover, du nom de ce premier patron du FBI américain, qui resta en poste 48 années et finit par voir des complots partout jusque dans son entourage.

5.2 Alerte

Le processus d'escalade doit absolument être formalisé : qui prévenir, dans quel ordre, par quels moyens de communication nominaux (et avec quels moyens de secours). Cela fait partie des livrables du DO de chaque MOA et en particulier de la DSI.

5.3 Qualification

Dans la mesure du possible, il importe de quantifier l'échelle de la crise. Un tableau d'échelle d'impact fait partie des livrables du DO du dispositif global, que chaque MOA pourra adapter si besoin (voir exemple en annexe).

Toujours dans la mesure du possible, annoncer assez rapidement une pré-évaluation du temps de traitement fait partie des fondamentaux de la communication de crise.

5.4 Traitement

Lors d'une crise, le premier réflexe des MOA est d'activer leur mode dégradé. Cela paraît facile à dire, mais on se retrouve rapidement confronté à des questions structurelles :

- qui doit décider de l'activation du mode dégradé ; certes il s'agit d'un choix interne à chaque MOA, ce qui suppose d'identifier dans les procédures de chaque MOA soit un responsable, soit un circuit de décision ;
- corollaire de la question précédente, qui doit décider du retour au mode nominal (mêmes contraintes de documentation et de responsabilité).

Schéma de la prise de décision T-FOR-DEC
Les secteurs soumis à des contraintes importantes telle l'aviation civile ont développé un modèle de prise de décision : le T-FOR-DEC

Temps : de combien de temps dispose-t-on ?

Faits : quelle est la situation objective ?

Options : quelles solutions s'offrent à nous ?

Risques : quels sont les bénéfices / risques de chaque option ?

Décision : prise de décision

Exécution de la décision

Contrôle et adéquation entre l'exécution, la décision et les risques

En termes de rôles pendant la crise, selon Christian MOREL (« Les décisions absurdes ») pendant une crise, ce sont les experts qui savent quoi faire, et la relation manager / expert est inversée. Les managers ont pour rôle essentiel de communiquer, d'organiser, et veiller à limiter les sollicitations externes des experts mais certainement pas de faire valoir une quelconque expertise technique (technique étant à entendre au sens large, qu'il s'agisse de compétences informatiques, médicales, biologiques, logistiques, juridiques, etc.).

L'ensemble des acteurs doivent garder en tête le triptyque précédemment évoqué temps / ressources / complexité. Face à une situation complexe et avec peu de ressources, il faut trouver / gagner du temps, face à une situation en temps et complexité contraintes il faut trouver des ressources, etc.

Le facteur humain est absolument majeur pendant une crise (relations entre les personnes, stress, etc.), et notamment le facteur fatigue humaine. Une crise qui dure 48h ne se gèrera pas, en termes de ressources et de fatigue, comme une qui dure 3 mois.

Crise longue, médecin requis

Dans le cas d'une crise qui s'étale sur des semaines ou des mois, il est indispensable de mettre à disposition de ceux qui sont au cœur du réacteur pour gérer la crise un médecin apte à dire si telle ou telle personne est dans un état physique compatible avec sa prise de poste ou s'il faut le renvoyer chez lui pour dormir quelques heures. Prévoir aussi des navettes, il ne faudrait pas rajouter à la crise des accidents contre des platanes en rentrant épuisé.

Les biais cognitifs sont un des pièges courants au sein des crises. Le sujet débord largement le cadre de cet opus mais il est nécessaire au management de connaître les principaux (biais de confirmation, biais de conformité, effet de halo, biais d'engagement, effet tunnel, effet de sidération).

D'expérience, le talon d'Achille de tout dispositif de gestion de crise est la communication, et en premier lieu les outils de communication. La messagerie électronique ne sera plus accessible, le téléphone bloqué sur certains sites, le Wifi coupé, les GSM seront dans certains bâtiments dans des cages de Faraday, etc. Prévoir un plan B, voire un plan C avec des outils basiques grand public est essentiel et doit faire partie de la documentation de chaque MOA (DO) et des tests (CHECK).

« Avec la présence massive de téléphones portables, les années 2020 sont largement favorables à des moyens de communications alternatifs et performants. »

Enfin, vouloir redémarrer le SI au plus vite n'est pas forcément une bonne idée. Tant que l'on n'a pas analysé précisément la cause de la crise, tant que l'on n'est pas sûr qu'il ne reste pas des méchants lutins cachés dans les coins, tant que l'on n'a pas la maîtrise des assets qui ont été touchés et de leur niveau de remédiation, tant que l'on n'est pas certain que le retour au mode nominal ne va pas se traduire par un nouveau passage en mode dégradé (pour certaines MOA telles les Urgences, c'est très pénalisant), alors on ne fait rien. Charge au Management d'encaisser la pression médiatique interne et externe.

PLAN BLANC NUMÉRIQUE : LA MINUTE D'APRÈS !

Par le Pôle d'Expertise Santé d'adista

Approche métier : Point de vue d'adista

Après le premier appel au support informatique, puis un deuxième... Le doute s'installe, la crédulité laisse vite place à l'évidence : le système d'information subit une attaque ! (Souvent en pleine nuit d'ailleurs).

« C'était attendu, nous le savions, nous le pressentions. Nous avons mis tout en

œuvre : les formations, les sensibilisations, les outils, les bons antivirus... ah non, pas tout le temps et pas sur tous les postes, tout a été mis à jour... ah non, pas tout, les exercices de crise, nous avons tout fait, tout envisagé... ».

Mais c'est violent, très violent pour tout le personnel de l'hôpital !

C'est la crise !



Tous les systèmes sont éteints, les accès internet sont coupés, voire les accès de téléphonie fixe, l'hôpital est confiné et complètement isolé.

Ça y est, on y est !

Le plan blanc numérique est enclenché.

Le Plan Blanc Numérique est un dispositif spécifique destiné aux établissements de santé pour faire face aux crises, en cas d'indisponibilité du système d'information,

y compris les cyberattaques. Ce plan, inspiré du Plan Blanc traditionnel (utilisé en cas de crise sanitaire), met l'accent sur la préparation et la réponse aux incidents numériques.

Nous n'allons pas, dans cet article, vous dérouler les très convenus processus d'une gestion de crise : La constitution de la cellule de crise avec les responsables, les équipes de réponse technique, les représentants des métiers, les responsables de la communication (interne et externe),

les représentants de la conformité et juridique, ainsi que les ressources humaines. Cette cellule va suivre le long chemin de la détection au retour à la normale en passant par les étapes d'évaluation, de réponse, d'investigation, de remédiation, de récupération et d'analyse post-incident.

Et le patient dans tout cela !

Bien que nous soyons une société de service numérique, nous n'allons pas aborder le sujet sous un angle « numérique » ou « informatique ». Au passage, l'Intelligence Artificielle n'aidera pas l'établissement privé de son système d'information, surprenant non ?

Le premier sujet qui doit être géré par l'établissement, c'est **la continuité des soins pour les patients** présents et le reroutage des urgences vers d'autres établissements. Pour pouvoir assurer la continuité des soins, il faut disposer rapidement des dernières informations à jour. Zéro papier ?

(NDLR : il y a de moins en moins de papier).

Beaucoup de services utilisent encore le papier ou impriment les données contenues dans le système d'information pour assurer la prise en charge et l'exécution de leurs lourdes tâches quotidiennes. Les imprimantes se font de plus en plus rares, l'usage du numérique est croissant, notamment via la dotation de tablettes. Digression (quoique) : j'ai toujours été étonné que dans les séries hospitalières américaines, chaque membre du personnel possède sa tablette et on voit souvent le chef de service de la chirurgie adapter et corriger le planning des chirurgiens sur un énorme tableau blanc avec feutre et effaceur...

Quelles sont les activités essentielles à maintenir en cas d'attaque cyber ?

En général, et surtout dans le milieu hospitalier, les activités essentielles sont connues et tombent sous le sens. En cas de crise, la réactivité et la coordination des soins sont mises à mal.



La cellule de crise qui assure le pilotage dans ces moments terribles doit avoir une vue d'ensemble de l'activité en cours et des services, ainsi que les différentes procédures pour pouvoir assurer les activités essentielles :

- **Soins :**

- Admission et triage
- Soins d'urgence (si maintenu)
- Soins intensifs
- Traitements et médicaments
- Chirurgie et interventions (ou le tableau Velléda est à jour)
- Suivi des patients hospitalisés
- ...

- **Gestion des Dossiers Médicaux :**

- Accès aux dossiers médicaux (format papier, PDF)
- Mise à jour des données

- **Coordination :**

- Accès aux canaux de communication inter-services
- Maintien des relations avec les organismes extérieurs, approvisionnement, équipements,

fournisseurs, transporteurs, etc.

- Soins à domicile

- **GTC et Sécurité :**

- Fonctionnement des équipements médicaux et procédures éventuelles sans informatique
- Fonctionnement des installations du bâtiment, accès, sécurité d'accès, etc.

- **Gestion des données et de la documentation :**

- Ai-je les bons documents pour les procédures dégradées ?
- Où sont-ils classés (pas sur les serveurs arrêtés j'espère !) ?
- Mes documents sont-ils à jour ?

La bonne posture !

L'attitude des participants d'une cellule de crise joue un rôle déterminant dans la gestion efficace et rapide d'une crise. Des comportements positifs tels que le calme, la collaboration, la communication claire et la responsabilité permettent de naviguer avec succès à travers des situations difficiles, assurant ainsi la continuité des opérations et la sécurité des patients et du personnel. Cependant, il est crucial de disposer des bonnes informations.



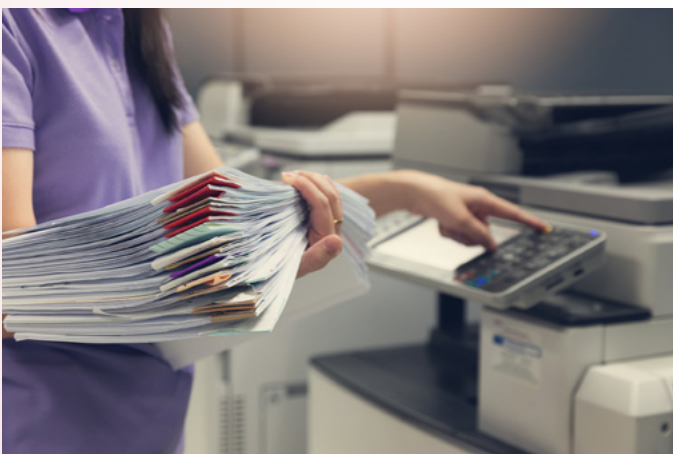
Les différents retours d'expérience sur ces cellules ont souvent confirmé ces comportements. Une fois que le mal est fait et la sentence tombée, l'humilité s'impose en matière de cybersécurité.

Lors des exercices cyber, le temps est court. Les cellules de crise simulent en quelques heures des jours entiers d'action

et de décision. Il est donc essentiel d'inclure dans la gestion de la crise la logistique de ravitaillement et les temps de repos nécessaires. Cela contribue fortement à des décisions éclairées et à une ambiance constructive et calme.

En attendant la remédiation et le retour au nominal : La procédure dégradée !

Nous l'avons constaté, la procédure dégradée est finalement un Plan de Reprise d'Activité (PRA) ou un Plan de Continuité d'Activité (PCA) manuel, utilisant des documents sous format papier ou électronique sous forme de fichiers. L'important est de disposer, au moment du "lockdown", des informations les plus à jour possibles, et surtout, de ne pas les stocker sur les serveurs informatiques de l'établissement ou sur des postes de travail connectés aux réseaux, car ils sont potentiellement vulnérables au piratage.



Pour ce faire, **adista** propose, dans le cadre de l'anticipation d'un arrêt brutal du système d'information de l'établissement, de mettre à disposition ses centres de données certifiés HDS et sécurisés, afin de sanctuariser les documents nécessaires à la procédure

dégradée.



L'établissement met à disposition, sur un serveur SFTP, les documents à jour tels que :

- Les dossiers patients au format PDF,
- Des dumps de bases de données,
- Des exports AD au format CSV,
- Les annuaires,
- Les procédures,
- Tout document nécessaire à la gestion de la crise et fournissant à la cellule de crise des informations à jour et pertinentes.

Le principe est qu'**adista** récupère ces informations de manière automatisée (avec un reporting à chaque transaction), les transactions sont sécurisées et vérifiées. Du côté de nos centres de données,

l'établissement n'a pas accès à ce sanctuaire en mode nominal ; **les accès ne sont ouverts qu'en cas de déclenchement du plan blanc numérique**. Les processus d'ouverture des accès sont consignés dans les procédures

communes et peuvent faire partie des exercices de crise. Une rétention des sauvegardes sur un minimum de 15 jours glissants est proposée de base.

La dissolution de la cellule de crise !

Le retour à la normale est maintenant stabilisé, les rapports sont complets, les leçons ont été tirées et des plans d'action pour le suivi et l'amélioration continue ont été établis, assurant ainsi que chacun sait ce qu'il doit faire.



Il est crucial d'acter et de communiquer la dissolution de la cellule de crise, sinon cela risque de devenir une histoire sans fin. Cependant, nous devons reconnaître que cette histoire n'a pas de fin définitive, car la menace cyber persiste. Même si le renforcement des mesures de sécurité nous permettra peut-être de déjouer avec succès une cyberattaque la prochaine fois, cela ne signifie pas que nous devons baisser notre vigilance.



En ces temps de célébration du 80ème anniversaire du débarquement, une citation nous vient à l'esprit :

« Le succès n'est pas final, l'échec n'est pas fatal : c'est le courage de continuer qui compte. » Winston Churchill

Nous remercions toutes les personnes avec lesquelles nous avons échangé sur le sujet qui nous ont inspirés cette solution par leurs retours d'expérience, elles se reconnaîtront : établissements, experts IT HDS adista, partenaires développeurs e-santé, professionnels d'établissements touchés par une cyber-attaque ou en posture de vigilance.



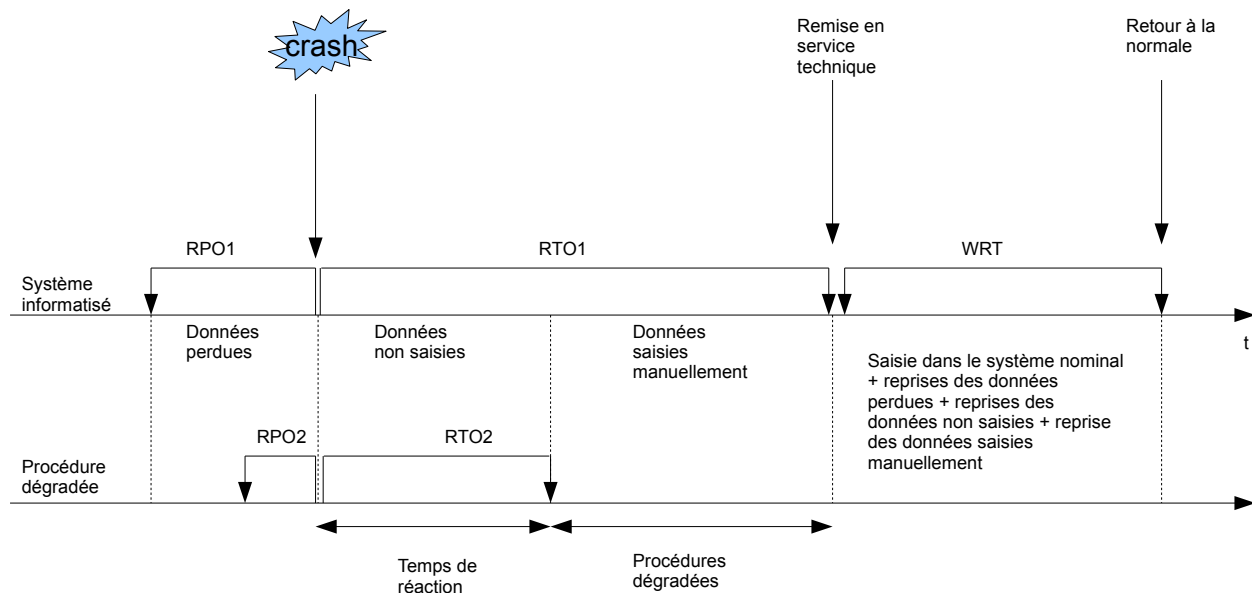
info.sante@adista.fr
www.adista.fr/secteurs/sante/

6. APRÈS LA CRISE

De la même façon qu'il faut déterminer et procéder la prise de décision de passer en crise, il faut aussi procéder la décision de retour à la normale : qui prend la décision ? selon quels critères ?

6.1 RTO et WRT

Remise en service après crash informatique



WRT : Work Recovery Time

RTO : Return Time Objective

RPO : Return Point Objective

Il est également important de bien faire la distinction entre le rétablissement de l'informatique (RTO : Return Time Objective) et le réel retour à la normale pour les MOA (WRT : Work Recovery Time). En effet dès que le SI est à nouveau disponible, il va falloir saisir tout ou partie des données perdues entre le moment de la panne et le passage en procédure dégradée (temps de réaction ou temps de sidération des MOA), et les données perdues pendant le temps de la

procédure dégradée (saisie papier la plupart du temps, donc saisies incomplètes). Le vrai retour au mode nominal peut prendre des heures, voire des jours dans les cas les plus complexes.

La stérilisation et le brancardage patient
Lors d'une panne du système informatisé de brancardage, la procédure dégradée consiste à rappeler des régulateurs humains et à transmettre les demandes de

courses par téléphone. L'historique importe peu et dès que le système est à nouveau fonctionnel, le retour en nominal peut être effectué. Dans ce cas précis RTO = WRT. En revanche, pour la stérilisation, le retour à la normale peut nécessiter de revoir toutes les compositions de boîtes de bloc opératoire : selon la configuration cette opération peut prendre des jours entiers.

Evidemment, il importe de s'assurer de la conservation des éléments techniques : ils serviront aux analyses post-mortem et dans le cas d'une attaque, ils seront nécessaires au dépôt de plainte.

6.2 Le REX

Le retour d'expérience (REX) suite à une attaque joue le même rôle que les tests de cellule de crise : le CHECK du PDCA. Il y a toujours des éléments qui ont bien fonctionné, mais d'autres moins bien ou mal, il importe que ces actions soient listées, partagées, analysées et rejoignent le ACT de la gouvernance générale du dispositif de crise cyber. Il est entendu que ces actions correctives concernent potentiellement à la fois le volet technique et le volet organisationnel du dispositif de crise, à la fois les MOA et la Direction Générale.

Maturité au regard des assureurs

Les assureurs du risque cyber ont tendance à considérer non pas le niveau précis de protection du système d'information du client, mais plutôt l'existence de processus formels de gestion et réduction des risques. Le rapport des REX est un grand classique des questionnaires assureurs.

6.3 La limite des assurances cyber

L'assurance coûte toujours cher avant le sinistre, mais en même temps assurer pour rien coûte encore plus cher. L'intérêt de l'assurance cyber ne réside pas dans le paiement d'une rançon suite à une attaque en ransomware (la législation varie sur ce point) mais dans les couvertures suivantes :

- la responsabilité civile de l'établissement en cas de dommage causé à un tiers à la

suite d'un sinistre cyber (cette garantie est exclue des couvertures RC classiques) ;

- la possibilité de faire appel à des équipes d'experts pour venir assister les équipes internes à l'analyse et à la remédiation ; certes un CHU (OSE ou OIV) pourra compter sur l'ANSSI, mais pas l'ensemble des 250 ou 300 gros établissements de santé sur le territoire ;
- la garantie de perte d'exploitation

financière pour interruption de service.

Mais l'assurance cyber a aussi deux conséquences positives:

- être assuré permet de ne pas être exposé en plus à un risque médiatique (« Et en plus ils n'étaient pas assurés »), même si ce dommage est difficile à chiffrer ;
- mais surtout, elle engage l'établissement à rentrer dans un cercle vertueux, l'assureur va exiger chaque année des plans de sécurisation, des dispositifs organisationnels de traitement et de réduction du risque cyber, etc.

Accessoirement, et c'est un élément dont les assurés tiennent rarement compte, appeler son assureur pour lui demander conseil sur un point relevant de la cyber (faut-il commencer par mettre à jour les OS des PC ou des serveurs en priorité ?) est un atout intéressant. En effet l'assureur est supposé avoir des statistiques précises sur tel ou tel risque : si les assureurs vous conseillent de mettre des serrures 3 points à votre porte d'entrée, c'est que leurs statistiques disent que la majorité des cambrioleurs passent par là. Se passer d'une telle manne d'informations semble pour le moins idiot, autant pour les cambriolages de domicile que des attaques cyber.

COMMENT DÉJOUER UNE CRISE CYBER ?

Par les équipes de Gatewatcher

Approche métier : Point de vue de Gatewatcher

Rennes, Villefranche-sur-Saône, Dax, Oloron-Sainte-Marie, Albertville, Arles, Castelluccio, Saint-Dizier, Vitry-le-François, Mâcon, Paris, Corbeil-Essonnes, Versailles... Cette courte liste n'est qu'un aperçu des établissements de santé publics et privés, sans distinction de taille, visés ces dernières années par des cyberattaques. À une époque où la technologie et l'automatisation ont colonisé de nombreux pans du « parcours de santé » tels que les dossiers patients informatisés (DPI), la gestion administrative médicale (GAM), la gestion économique et financière (GEF), les dispositifs médicaux connectés (IOT) et les systèmes de télémedecine, la cybersécurité est devenue un pilier indispensable garantissant la sécurité et la confidentialité des données critiques.

L'hyper-connectivité, censée simplifier notre vie, accroît paradoxalement notre vulnérabilité aux attaques. À l'ère du « tout numérique », transmettre ses données personnelles aux géants du numérique n'est plus un choix mais un prérequis. Nouvel « or noir » du XXI^e siècle, elles ne sont pour autant pas sans danger au vu de leur exploitation frénétique et deviennent une cible de choix pour les cybercriminels, transformant la cybersécurité en un pilier fondamental de notre intégrité et de notre bien-être. Cinquième secteur d'activité le plus ciblé à l'échelle européenne (ENISA, 2023), la santé fait face à des cyberattaques toujours plus fréquentes et plus sophistiquées, visant en particulier les systèmes d'information hospitaliers (SIH).

Qu'est-ce qu'une crise d'origine cyber ?

Au cœur de la cybersécurité, une crise cyber représente un événement où l'intégrité, la confidentialité ou encore la disponibilité d'un système d'information est gravement menacée. Dans le domaine de la santé, les enjeux sont particulièrement élevés - une violation peut faire la différence entre la vie et la mort. Bien plus que de savoir si une attaque aura lieu, la posture appropriée

est d'évaluer son niveau de préparation face à son inéluctable survenue. Il s'agit moins d'une question de possibilité, que de temporalité et de moyens mis en œuvre pour nous y préparer. Face à ce défi, il devient crucial de reconsidérer notre approche à la cybersécurité, en passant d'une posture essentiellement réactive à une approche proactive « by design ».

Prévoir pour prévaloir : anticipation et détection.

La force de l'attaquant réside dans le facteur temps. C'est une caractéristique inhérente par rapport aux défenseurs : l'un agit tandis que l'autre réagit. Pour minimiser le risque et reprendre le contrôle sur un contexte

cyber moins incertain, il est recommandé d'adopter certaines pratiques. La préparation à une crise cyber s'ancre autour de deux piliers fondamentaux : l'anticipation et la détection.

Anticipation : quatre points clés de la proactivité

Anticiper une cyberattaque dans le secteur de la santé n'est pas une tâche aisée, mais elle est impérative. Cela commence par une **connaissance** exhaustive du paysage technologique existant : connaître le champ de bataille avant la guerre. Il faut donc être capable de cartographier le réseau, de comprendre l'interopérabilité entre les systèmes, d'identifier où résident les actifs critiques, telles que les données sensibles, etc. Mais anticiper va au-delà de la simple connaissance technique ; cela implique également de se familiariser avec les menaces actuelles et émergentes. La deuxième étape se profile donc tout naturellement : une **évaluation des menaces** à travers des tests de pénétration réguliers. Le pentesting se révèle être un précieux allié, mettant en lumière les vulnérabilités et fournissant des renseignements sur les vecteurs d'attaque potentiels. Puis, intrinsèquement liée aux menaces : **l'évaluation des risques**. Non pas pour tout verrouiller, mais pour savoir où les renforcements de défense sont le plus nécessaire. Principe fondamental en cybersécurité, le risque peut être grossièrement calculé en combinant les actifs, les menaces et les vulnérabilités connues. Cependant, pour une hiérarchisation plus précise, il est prudent d'intégrer l'impact, agissant comme un multiplicateur de risque. Cela revient à classer les risques par ordre de priorité. Un risque avec une probabilité élevée mais un impact faible serait considéré comme moins critique et serait rangé plus bas dans la liste des priorités. En revanche, les risques avec une probabilité plus faible mais un impact élevé seraient favorisés dans cette évaluation.

Prenons un hôpital qui utilise un système informatisé pour gérer les stocks de médicaments essentiels et considérons deux

risques potentiels :

- **Risque 1** : La gestion des stocks de médicaments est corrompue due à une cyberattaque. Bien que la probabilité de cette attaque soit modérée, l'impact potentiel est relativement faible, car les informations concernant les stocks peuvent être récupérées à partir de sauvegardes et des mesures de sécurité peuvent être mises en place pour empêcher une récurrence.
- **Risque 2** : Le système informatisé de gestion des stocks de médicaments est paralysé suite à une cyberattaque, empêchant ainsi le personnel médical d'accéder aux informations sur les médicaments disponibles. Bien que la probabilité de cette attaque soit faible en raison des mesures de sécurité en place, l'impact potentiel est extrêmement élevé, car cela pourrait entraîner des retards dans l'administration de médicaments vitaux aux patients, mettant ainsi leur vie en danger.

Quand bien même le premier risque est plus susceptible de se produire, il est considéré comme moins critique en raison de son impact relativement faible sur la prestation des soins aux patients. L'hôpital devrait donc accorder une attention particulière à la prévention et à la mitigation du deuxième risque.

Dernier point clé, compte tenu des facteurs précédemment évoqués, il est impératif de mettre en place un **plan de continuité des activités** (PCA) qui détermine clairement les responsabilités de chacun. Cela inclut les procédures, ainsi que les assignataires. En effet, une cellule de crise doit être pluridisciplinaire car elle ne relève pas uniquement de la technique mais aussi de la communication, de la finance, des ressources

humaines, etc. L'adage « mieux vaut prévenir que guérir » semble ainsi particulièrement pertinent.

Détection : savoir que l'on est ciblé

Si l'anticipation est la première ligne de défense, la détection est le système d'alerte précoce. À l'instar d'un dépistage qui permet d'identifier les maux avant qu'ils ne s'aggravent, la détection cyber offre la possibilité de repérer les anomalies dès leur apparition. Dans un paysage législatif en perpétuelle évolution, comme avec l'implémentation imminente de la directive européenne NIS2, toutes les Organisations d'Importance Vitale (OIV) et Opérateurs de Services Essentiels (OSE), à terme Entités Essentielles (EE), sont désormais tenus de mettre en place une gestion de crise cyber. Cette démarche devient incontournable, notamment lorsque les menaces extérieures sont liées à des événements d'importance majeure comme les Jeux Olympiques. Certaines solutions permettent précisément de combiner obligation et opportunité, offrant ainsi une protection accrue. Olivier Pedurand, RSSI du SIB reconnaît que « *le cadre réglementaire permet de faire évoluer positivement le niveau de sécurité. Le fait d'avoir une contrainte européenne permet*

de sanctuariser les moyens alloués à la SSI ». De plus, « *les sondes NDR permettent en partie de répondre à cet aspect réglementaire* ». Outre les obligations conjoncturelles, le secteur doit également prendre en compte ses limites structurelles. Les hôpitaux rencontrent majoritairement trois grandes contraintes : la faible culture du risque cyber chez le personnel soignant, un budget souvent restreint et un spectre technologique particulier.

Dans un monde idéal, nous bloquerions chaque attaque avant qu'elle n'atteigne nos systèmes. Cependant, dans la réalité, certaines attaques passeront inévitablement au travers des mailles du filet. C'est ici qu'intervient la détection : la capacité de reconnaître rapidement une intrusion ou une activité suspecte pour y répondre de manière efficace. Le NDR - Network Detection & Response - excelle là où les défenses traditionnelles fléchissent, offrant une visibilité inégalée sur le trafic réseau, identifiant ainsi les anomalies.

Le NDR, stéthoscope et scalpel du réseau

En effet, le NDR occupe une place prépondérante dans la protection des infrastructures critiques de santé. Il garantit une couche supplémentaire de sécurité et particulièrement lors des phases préliminaires d'anticipation et de détection des menaces. Sa capacité à se focaliser, entre autres, sur la sécurité biomédicale constitue un avantage majeur, notamment face à la montée en puissance des dispositifs

médicaux connectés et des advanced persistent threats (APT). Etant donné que la majorité des attaques se produisent sur les réseaux, le rôle du NDR va au-delà de la simple prévention, il devient un élément indispensable. Olivier Pedurand l'affirme : « *les sondes réseaux font maintenant partie du socle de base à déployer pour la sécurisation d'un SI comme un firewall, un proxy, un antivirus ou un EDR* ». Son paramétrage

individuel qui se déploie sur l'ensemble de l'hôpital en des points uniques et bien identifiés permet une surveillance pointue et exhaustive des appareils, même ceux non répertoriés par la direction informatique, sans perturber les Systèmes d'Information Hospitaliers (SIH). Il identifie l'ensemble des appareils connectés au réseau informatique de l'hôpital : postes de travail, machines médicales, smartphones, objets connectés, et prévient dès les premiers signaux faibles d'une cyberattaque, réduisant ainsi les impacts métiers et les répercussions sur les patients. En effet, un risque cyber avéré et observé par les RSSI de divers hôpitaux est lié à la convergence entre les technologies de l'information (IT) et les technologies opérationnelles (OT). Grâce à son approche multi-vectorielle, couplée à l'intelligence artificielle (IA) et au Machine Learning (ML), le NDR offre une solution de

détection et d'identification inégalée, même sur les flux chiffrés, tout en garantissant la confidentialité des données : celles-ci demeurent sous la propriété exclusive des Centres Hospitaliers Universitaires (CHU) ou des Centres Hospitaliers Publics (CHP). À une époque où les données personnelles sont un véritable joyau et un enjeu de souveraineté, Vincent Trély, président de l'APSSIS, déclarait au micro du podcast « Dans l'œil de la cyber » qu'il y a « *une nette accélération sur l'usage de sonde, NDR, XDR, monitoring réseau, SOC etc. Et cela va être extrêmement dynamique sur les années qui viennent* ».

D'autre part, les initiatives étatiques telles que « CaRE », soulignent bien que « le cyber n'est plus une variable d'ajustement » ; une impulsion est nécessaire pour promouvoir une cyber-résilience des établissements hospitaliers.

Vers une santé numérique résiliente

La cyber proactivité est le fil conducteur de la stratégie de défense efficiente. C'est l'alliance entre la préparation et la prévention. En embrassant des solutions telles que le NDR pour contrer les attaques réseau, nous préservons les avantages de la numérisation tout en sécurisant nos structures médicales. En définitive, dans cette lutte constante pour la sécurité et la résilience du secteur médical

face aux défis numériques, rappelons-nous la sagesse d'Hippocrate : '*Primum non nocere*' - d'abord, ne pas nuire. En adoptant des pratiques de gestion de crise robustes, nous pouvons non seulement anticiper les dommages, mais aussi affirmer notre engagement envers le bien-être et la sécurité des patients, un devoir essentiel.



www.gatewatcher.com

7. CONCLUSION

La cyber, ce n'est ni un logiciel ni un matériel, c'est une démarche globale.

Il en est de même pour la gestion de crise : il s'agit d'une démarche globale qui touche toutes les strates hiérarchiques d'une entreprise, qui touche moins la technique que les processus, et qui s'inscrit dans un cadre global d'amélioration continue - on n'est pas résilient à la naissance, on le devient.

Le cadre global reste toujours la roue de Deming PDCA - c'est ce que l'aviation civile fait depuis 70 ans et cela fonctionne, la preuve étant qu'il s'agit d'un des moyens de transport les plus sûrs du monde.

Démarche PDCA, sponsoring de plus haut niveau, approche processus, le tout sans quasiment aucun investissement matériel ou logiciel et seulement de l'huile de coude. Comme pour beaucoup de sujets qui touchent à la cyber, c'est d'abord de l'organisation et du bon sens.

LE KIT PCRA : CONTENUS ET OBJECTIFS

Par les équipes de l'Agence du Numérique en Santé

Approche métier : Point de vue de l'Agence du Numérique en Santé

Le programme CaRE « Cybersécurité accélération et Résilience des Établissements » a pour objectif de renforcer la cybersécurité des établissements sanitaires et médico-sociaux. Depuis décembre 2022, la Délégation au Numérique en Santé (DNS) et l'Agence du Numérique en Santé (ANS) coordonnent la Task Force Cyber qui regroupe les acteurs clefs de la cybersécurité dans le secteur de la santé. L'ensemble des travaux de cette Task Force est conduit de manière collaborative avec les acteurs de l'écosystème (fédérations hospitalières et médico-sociales, industriels).

Le programme CaRE décline ainsi un plan d'action concret et ambitieux pour la période de 2023 à 2027.

Le programme se décline en 4 axes :

- Gouvernance et résilience
- Ressources et mutualisation
- Sensibilisation
- Sécurité opérationnelle

Dans le cadre de l'axe Gouvernance et résilience, l'un des objectifs est de préparer

et accompagner les établissements à réagir et à faire face à la cybermenace, les rendre plus résilients et mieux préparés en cas d'incident cyber. Les enjeux de cybersécurité et la gouvernance associée doivent ainsi être pris en compte par les établissements. Ces derniers doivent pouvoir s'approprier, décliner et déployer le programme CaRE au cœur de leur projet d'établissement et le rendre visible au travers de leurs choix stratégiques et budgétaires.

L'action 3 « Préparer et accompagner les établissements à réagir et à faire face à la menace » de cet axe Gouvernance et résilience fixe l'objectif d'inciter les établissements à poursuivre la dynamique de campagne de réalisation des exercices de crise et également de formaliser des Plans de Continuité et de Reprise d'Activité (PCRA). Cette démarche préventive permet à l'établissement de mieux connaître son organisation, et de définir les activités qui sont pour lui essentielles ainsi que les étapes à suivre précisément en cas de survenue d'une crise.

Pourquoi un kit PCRA ?

Dans la continuité des travaux réalisés pour produire et déployer les kits d'exercices de crise, les établissements sanitaires et leurs représentants ont exprimé la volonté d'approfondir la démarche et d'être accompagnés dans la formalisation et la mise en œuvre de leur plan de continuité

d'activité et de leur plan de reprise d'activité. L'élaboration d'un PCRA par un établissement peut représenter un défi de taille, nécessitant la mobilisation de la direction générale et des référents métiers et supports pour permettre une bonne appropriation à tous, quel que soit le domaine d'expertise exercé

au sein de l'établissement.

La mise à disposition d'un kit PCRA clé en main va permettre d'aider l'établissement, d'un point de vue méthodologique, dans sa démarche de production et de mise en œuvre d'un PCRA.

Une première version du kit a été construite avec la Task Force, les fédérations et leurs représentants métiers et des experts lors d'ateliers de conception puis mise à disposition en septembre 2023. Une phase pilote a été organisée de septembre à fin 2023 pour tester ce kit en établissement. Cette phase pilote a montré une forte mobilisation des établissements avec 28 établissements engagés. Le choix des établissements participant à cette phase pilote a été fait de manière à obtenir une grande hétérogénéité : du secteur public comme privé, de taille diversifiée, et localisés dans plusieurs régions de France.

C'est par le biais de cette diversité et de l'implication forte des représentants de ces établissements qu'un outil méthodologique générique, simple, et facilement adaptable aux spécificités de chacun a pu être construit. Ce pilote a également permis d'identifier les difficultés rencontrées par les établissements, et les bonnes pratiques pouvant être mises en place pour construire le PCRA de l'établissement.

Ces travaux ont démontré l'intérêt de donner un guide méthodologique pour accompagner les établissements dans cette mission de production des PCRA et de soutenir toutes les démarches en ce sens.

15 établissements ont nommé un responsable PCRA, 17 ont constitué une instance de suivi des travaux et 39 Bilans d'Impact d'Activité (BIA) ont été réalisés par 15 établissements de santé sur ces 3 mois de phase pilote.

Établissements qui ont participé à la phase pilote	Établissements qui ont nommé un responsable PCRA	Établissements qui ont constitué une instance de suivi des travaux	Bilans d'Impact d'Activité (BIA) réalisés
28	15	17	39



A l'issue, la mise à jour du kit, prenant en compte les retours des « testeurs » a pu être proposée rapidement : elle est aujourd'hui disponible publiquement sur le site de l'ANS pour un accompagnement du déploiement en 2024.

Dans la continuité et pour favoriser son

appropriation, l'équipe intégrant les collaborateurs de l'ANS et les experts du CHU de Lille, a animé un [webinaire de présentation du kit PCRA](#) le 15 mars 2024.

Le contenu du Kit PCRA

S'appuyant sur la documentation de référence ([Plan Blanc Numérique](#) de la DGOS, [guide de la continuité](#) d'activité du SGDSN) et adoptant une approche orientée métier, la mise en place de ce kit permet de garantir la continuité des différents métiers (soins, administratifs, supports) d'un établissement avec une démarche qui concerne toutes les fonctions d'un établissement (pas uniquement les systèmes d'information) en couvrant 4 scénarios d'indisponibilité (ressources humaines, SI, bâtiments, prestataires/fournisseurs).

Ce kit est divisé en 4 parties :

- Le cadrage du projet : ensemble de documents permettant d'initier la démarche (mode d'emploi du kit, document de cadrage projet, lexique, fiche de mission pour le Responsable PCRA) ;
- La méthodologie : ensemble de documents permettant d'appréhender la méthode de rédaction des plans de conduite et reprise d'activité (fiches, prototype de BIA, trame de PCRA...) ;
- La gestion du PCRA : documents expliquant comment maintenir à jour son PCRA dans le temps (MCO du PCRA, grille d'évaluation du PCRA) ;
- Des exemples de BIA.

Le [Kit est disponible](#) sur le site de l'ANS.

Faciliter la mise en œuvre de la démarche via des financements dédiés

Le déploiement du kit PCRA dans le cadre du plan d'action CaRE s'inscrit dans la continuité des initiatives précédentes lancées dès 2012 avec le programme Hôpital numérique puis le programme HOP'EN depuis 2019, qui demandent aux établissements de santé de mettre en place un plan de reprise d'activité du système d'information formalisé et testé. Ces indicateurs historiques sont d'ailleurs repris dans les critères d'évaluation numériques du manuel de certification HAS qui précise dans sa version 2024 que les établissements doivent déployer un plan de

continuité d'activité et un plan de reprise d'activité dans tous les secteurs.

L'objectif est d'impliquer l'ensemble des équipes opérationnelles des établissements et de les mobiliser sur la définition du PCRA. Ce travail collectif permet notamment de sensibiliser les directions et les Présidents de Commissions Médicales d'Etablissement. Un domaine « Stratégie de continuité et de reprise d'activité », est en cours de co-construction dans le cadre de l'axe 4 du plan d'action CaRE « Sécurité opérationnelle ». Ce domaine, construit de façon collaborative

avec l'ensemble des contributeurs des établissements qui souhaitent s'associer aux travaux et avec les fédérations, se concentre sur deux sujets que sont la sauvegarde et la continuité et reprise d'activité. Ce domaine s'inscrit dans la continuité des travaux initiés par les précédents programmes numériques et permettra de fournir aux établissements les financements nécessaires à la mise en place des solutions de continuité et de reprise d'activité en atteignant les objectifs fixés par le domaine sur ce volet.

Le lancement de ce domaine est prévu sur le quatrième trimestre 2024.

De même, dans le cadre de la mise en place

des Centres Régionaux de Ressources Cyber (CRRC), l'un des objectifs fixés à ces CRRC est l'accompagnement des établissements dans le déploiement du kit méthodologique national de PCRA proposé dans le cadre du programme CaRE.

Enfin, une démarche de co-construction avec des Etablissements et Services Sociaux et Médico-Sociaux (ESSMS) est également en cours pour adapter et décliner ce kit au secteur médico-social et permettre à ces établissements de se doter d'un PCRA adapté à leurs activités. L'ambition est de publier une version du kit PCRA adaptée aux ESSMS en juillet 2024.



CaRE Programme national de renforcement Cybersécurité

8. LES 11 COMMANDEMENTS

Commandement 1 :

désigner un pilote de la démarche globale, qui soit officiellement adoubé par la Direction Générale et qui ait les mains libres.

Commandement 2 :

devenir résilient est un chemin perpétuel ; c'est une dynamique et non pas un état.

Commandement 3 :

la fréquence des tests est plus importante que leur périmètre.

Commandement 4 :

le besoin de résilience touche tous les services et processus métier sans exception. La DSI n'est qu'un des acteurs parmi d'autres.

Commandement 5 :

commencer par les fonctions support critiques au soin ; elles montreront l'exemple pour les autres.

Commandement 6 :

établir une cartographie de vos interlocuteurs externes (ANSSI, GRADE, ARS, GHT, etc.) pour savoir qui fera quoi, qui pourra aider, qui vous devrez alerter au moment de la crise. Et nommez un responsable de cet annuaire, qui va devoir être régulièrement vérifié.

Commandement 7 :

établir une procédure claire de quoi couper en priorité en cas de crise et dans quel ordre. Cela tient en 2 pages maximum, et ce doit être accessible à tout moment.

Commandement 8 :

prévoir des moyens alternatifs de communication, a minima avec Tchap et Signal (Whatsapp doit être réservé à un usage privé). Et tenez à jour des salons et listes de diffusion dans ces applications. Dans une crise, le premier facteur de stress est l'impossibilité de se joindre.

Commandement 9 :

avant, pendant et après la crise, la personne providentielle n'existe pas. Seul le travail d'équipe compte.

Commandement 10 :

la phase de REX est primordiale. Ne pas la dérouler dans les règles de l'art est le meilleur moyen de compromettre les chances de survie de l'organisation à la prochaine crise.

Commandement 11 :

chaque MOA doit prévoir une liste de ses interlocuteurs externes, à prévenir en cas d'attaque cyber de la structure. Si un CHU est attaqué, il faudra prévenir l'Université, la Ville, les promoteurs de recherche clinique, etc.

9. ANNEXES

	Synthèse	Activité	Financier	Conformité	Image	Juridique	Vie privée
1- Faible	La structure surmontera les impacts malgré quelques difficultés	Impact sensible, contournement possible occasionnant une gêne supportable	Perte inférieure à 0,001% du budget	Non conformité mineure, avertissement de la CNIL et de la HAS	Dégrader temporairement l'image de l'ES au niveau régional. Parution dans la presse régionale. Connaissance de l'incident par les instances régionales.	Réclamation non contentieuse. Plainte classée sans suite.	Les personnes concernées ne seront pas impactées
2- Moyen	La structure surmontera les impacts avec de sérieuses difficultés	Impact important, mise en place des procédures dégradées, rappel de personnels. L'activité est ralentie tout ou partie.	Perte entre 0,001% et 0,01% du budget	Non conformité majeure, sanction administrative de la CNIL	Dégrader temporairement la réputation de l'ES au niveau national. Parution dans la presse nationale. Connaissance de l'incident par les instances nationales.	Réclamation indemnitaire. Infraction passible d'une amende.	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés
3- Important	La structure surmontera les impacts avec de très grandes difficultés	Arrêt de tout ou partie de l'activité malgré la solution de remplacement	Perte entre 0,01% et 0,1% du budget	Interdiction temporaire d'exercer l'activité, non autorisation de la CNIL pour un traitement	Dégrader durablement la réputation de l'ES au niveau national.	Réclamation indemnitaire ou réclamation pénale. Causer une infraction passible d'une sanction pénale.	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives
4- Critique	La structure peut disparaître tout ou partie	Arrêt total de l'activité	Perte supérieure à 0,1% du budget	Interdiction définitive d'exercer l'activité	Dégrader durablement la réputation de l'ES au niveau mondial.	Réclamation pénale. Causer une réclamation passible des assises.	Les personnes concernées pourraient connaître des conséquences significatives, voire irréversibles, qu'elles pourraient ne pas surmonter

10. RESSOURCES

Concernant les facteurs humains, le meilleur ouvrage que j'ai pu trouver est, sans surprise, issu de l'aéronautique : « *Le pilote acteur de sa sécurité* », Frédéric Bertrand, Editions Cépadues.

Concernant la sociologie du traitement des risques, on trouve entre autres :

« *Les décisions absurdes. Sociologie des erreurs radicales et persistantes* », Christian MOREL, Paris, Gallimard, coll. « Bibliothèque des sciences humaines », 2002

« *L'inquiétant principe de précaution* », Gérald BRONNER

« *Vous allez commettre une terrible erreur* », Olivier SIBONY

(Ce dernier ouvrage constitue d'ailleurs une très bonne introduction à l'illustration de la notion de biais cognitifs)

Pour ce qui concerne les tests de cellule de crise, l'ANS met à disposition des kits en 3 versions (débutant / intermédiaire / confirmé) : <https://esante.gouv.fr/strategie-nationale/cybersecurite>.

L'ANSSI met également à disposition certains kits sectoriels : <https://cyber.gouv.fr/actualites/gestion-de-crise-lanssi-met-disposition-des-kits-dexercices-sectoriels>



Association Pour la Sécurité des SI de Santé

 84 rue du Luart
72160 Duneau

 06 29 36 59 95

 secretaire@apssis.com

www.apssis.com



Licence du document

Auteur : Cédric CARTAU

Ce document est sous licence Creative Commons BY-NC-ND-SA :

- BY : attribution de l'auteur initial
- NC : interdiction de tirer un profit commercial
- ND : impossible d'intégrer le document dans une œuvre composite
- SA : partage de l'œuvre, avec obligation de rediffuser selon la même licence ou une licence similaire (version ultérieure ou localisée)