Directeur d'hôpital

Promotion : **2022-2023**

Date du Jury : **octobre 2023**

Cyberattaques en établissement public de santé : anticiper les conséquences de l'inéluctable

Diane VERES

Remerciements

Mes remerciements s'adressent tout d'abord à l'équipe de direction du Centre hospitalier universitaire (CHU) de Reims m'ayant accordé toute la confiance et les ressources nécessaires à la réalisation de ce mémoire. Une pensée toute particulière pour Madame Laëtitia MICAELLI-FLENDER, Directrice générale, Madame Hélène OPPETIT, Directrice générale adjointe et Madame Lucie DELECRAY, Secrétaire générale mais aussi référente de stage, qui ont su démontrer un intérêt particulier pour cette réflexion.

Je remercie également l'ensemble des professionnels rencontrés durant mon stage et interrogés à distance dans d'autres établissements pour leur disponibilité ainsi que nos échanges riches d'enseignements et de perspectives encourageantes.

J'adresse toute ma reconnaissance à Monsieur Cédric CARTAU, Responsable de la sécurité des systèmes d'information du CHU de Nantes, qui a su m'expliciter avec une pédagogie sans faille la technicité du sujet cyber et m'accompagner dans la rédaction de ce mémoire.

Enfin, je souhaite remercier l'équipe administrative et pédagogique de l'Ecole des Hautes Etudes en Santé Publique (EHESP) pour la qualité des supports documentaires mis à disposition et leur accompagnement m'ayant permis de proposer ce travail de recherche appliqué à un établissement public de santé.

Sommaire

Liste des sigles utilisés

ANS	Agence du numérique en santé
ANSSI	Agence nationale de sécurité des systèmes d'information
AQSSI	Autorité qualifiée pour la sécurité des systèmes d'information
ARS	Agence régionale de santé
CCH	Cellule de crise hospitalière
CME	Commission médicale d'établissement
DGOS	Direction générale de l'offre de soins
DGS	Direction générale de la santé
DIM	Département de l'information médicale
DMP	Dossier médical partagé
DPI	Dossier patient informatisé
DSI	Direction des systèmes d'information
GHT	Groupement hospitalier de territoire
HDS	Hébergeur de données de santé
HRO	*High Reliability Organization* / Organisation à haute fiabilité
NTIC	Nouvelles technologies de l'information et de la communication
OPSSIES	Observatoire permanent de la sécurité des systèmes d'information des établissements de santé
OSE	Opérateur de service essentiel
PCA	Plan de continuité d'activité
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PMSI	Programme de médicalisation des systèmes d'information
PRA	Plan de reprise d'activité
PSSI	Politique de sécurité des systèmes d'information
RETEX	Retour d'expérience
RGPD	Règlement général sur la protection des données
RSSI	Responsable de la sécurité des systèmes d'information
SDSI	Schéma directeur des systèmes d'information
SIE	Système d'information essentiel
SIH	Système d'information hospitalier
SSE	Situations sanitaires exceptionnelles

Introduction

« Un terrain de guerre », « une onde de choc », « le chaos », c'est ainsi que Docteur Jean Fabre, chef du service d'accueil des urgences du Centre hospitalier de Dax, a débuté le retour d'expérience portant sur la cyberattaque informatique ayant frappé son établissement le 9 février 2021.

Matérialisation d'une nouvelle forme de malveillance et délinquance permise grâce à l'essor de l'utilisation de l'outil informatique depuis les années 1980, les cyberattaques en établissements publics de santé s'inscrivent dans l'actualité de la cybercriminalité. Les premiers virus informatiques (annexe 1), créés aux fins d'extorsion de données sensibles dans le secteur militaire, ouvrirent la voie à une abondante réglementation nationale et européenne portant sur la sécurisation des systèmes d'information. Ainsi, la loi Godfrain avait su poser, dès sa publication le 5 janvier 1988, les jalons de la protection des nouvelles technologies de l'information et de la communication (NTIC), notamment en réprimant les actes de criminalité informatique. Elle fut ultérieurement complétée par la loi pour la confiance dans l'économie numérique du 21 juin 2004 ajoutant une sanction pénale en cas de failles informatiques non publiées ou fournies à des tiers. Concomitamment se sont également multipliés les moyens d'agir des utilisateurs sur leurs données informatisées par la loi Informatique et Libertés du 6 janvier 1978 successivement complétée par des transpositions du droit européen (RGPD) et décrets d'application. Finalement, l'Union européenne a adopté une stratégie plus offensive en misant sur des références harmonisées de niveaux de sécurité des systèmes d'information dans ses pays membres. Les établissements supports de nos Groupements Hospitaliers de Territoire (GHT) sont ainsi entrés dans la loi de programmation militaire en qualité d'opérateur de service essentiel (OSE) et bénéficient désormais de l'accompagnement de nombreuses agences nationales (ANSSI, ANS, CERT-Santé, *etc*.) pour parfaire leurs infrastructures.

Pour autant, les établissements publics de santé sont aujourd'hui victimes d'une typologie d'attaque sans précédent, capable d'impacter simultanément les trois piliers de la cybersécurité que sont la disponibilité, l'intégrité et la confidentialité des données. La première occurrence avérée de ce phénomène date ainsi du 5 février 2016, au *Hollywood Presbytarian Medical Center* de Los Angeles aux Etats-Unis. Il fut le premier établissement de santé touché, par un *ransomware* ou rançongiciel (annexe 1) générant une paralysie de ses systèmes d'information. Dépassant l'unique question technique de sécurisation des infrastructures informatiques, l'établissement avait alors accepté de régler la rançon demandée afin de limiter toute perte de chance pour les patients.

En effet, dans la situation la plus défavorable, l'arrêt soudain de l'ensemble du parc informatique de la structure empêche la continuité de la prise en charge des patients admis, programmés ou non programmés. Les données antérieurement saisies sont inaccessibles et les outils connectés d'explorations médicales illisibles. Les moyens de communication internes comme externes ne fonctionnent plus. A ce tableau chaotique se greffe enfin le vol des données personnelles des patients par le cybercriminel.

L'année 2021 a été le théâtre de l'expansion du nombre de cyberattaques touchant les établissements de santé français (OPSSIES, 2023) et, à l'instar du terme de « crise sanitaire » employé durant la pandémie de COVID-19, l'expression de « crise cyber » a pu s'imposer. L'ANSSI privilégie pourtant la sémantique de « crise d'origine cyber ». En effet, la cyberattaque ne peut être considérée comme une crise en soi. Elle ne sera que le facteur d'une déstabilisation de l'organisation pouvant générer une crise. Comme le souligne Laurane Raimondo, la crise est « un moment de rupture de la linéarité impliquant une prise de décision à même de modifier durablement les mécanismes sur lesquels fonctionne la personne, le groupe ou l'organisation » (Raimondo, 2022 :17).

L'anticipation des conséquences d'une cyberattaque ne peut donc reposer sur une simple sécurisation des systèmes d'information de nos établissements publics de santé. Nombre d'acteurs de la cybersécurité s'accordant aujourd'hui à souligner que la question n'est plus de savoir si nous serons cyberattaqués mais quand. Il s'agit en réalité de questionner la fiabilité et la résilience de nos organisations face à cette menace, au-delà des infrastructures et dispositifs techniques de sécurisation. La prévention du risque doit à ce titre inclure l'anticipation des conséquences.

Dans ce contexte mêlant technicité du risque et généralité de ses conséquences, comment un établissement public de santé peut-il organiser sa résilience ? Quels outils peut-il mobiliser pour anticiper les conséquences d'une crise d'origine cyber ?

Fruit d'une réflexion professionnelle de plusieurs mois aux fins de réalisation d'exercices de préparation à la survenue d'une cyberattaque, la méthodologie de recherche sera présentée en préambule d'un développement proposant d'aborder les éléments utiles à la compréhension des cyberattaques et leurs conséquences en établissement public de santé (1) et les outils actuellement mobilisables d'anticipation de la crise d'origine cyber (2) dont l'analyse permettra d'être force de préconisations dans l'investissement du risque cyber aux fins de gain en fiabilité et résilience (3).

Méthodologie de recherche

A) Contexte de l'étude

Le stage professionnel faisant partie intégrante de la formation d'élève-directeur d'hôpital a rapidement été l'occasion de pouvoir m'intéresser aux enjeux numériques d'un établissement public de santé. Entre convergence des systèmes d'information du GHT et menace grandissante des cyberattaques répétées durant l'année 2021-2022, la nécessité de réaliser un test des cellules de crise au CHU de Reims se faisait prégnante et pouvait constituer une mission adaptée temporellement à la durée du stage professionnel. S'ajoutait également la volonté de la DSI du CHU de Reims de pérenniser des exercices au sein des unités opérationnelles de l'établissement, sans perdre de vue la dimension GHT. Le choix fut ainsi arrêté pour l'année 2023 : des exercices organisés avec des ressources internes au sein de l'établissement support et une mise en conformité réglementaire de test des cellules de crise via l'appel à projet régional pour les établissements parties au GHT. Ma réflexion portant sur le mémoire de fin de cycle de formation d'élève-directeur d'hôpital s'orienta alors vers la recherche des outils permettant d'anticiper les conséquences d'une cyberattaque.

B) L'observation d'une entité ministérielle sensible à l'occasion du stage extérieur

Le stage extérieur s'établissant pour ma promotion entre deux périodes de stage professionnel, l'occasion me fut donnée d'intégrer durant deux mois la Direction du Numérique du Ministère de l'Europe et des Affaires Etrangères (MEAE). Ce premier terrain d'observation me permit de prendre connaissance du fonctionnement cyber en administration centrale disposant de nombreux sites extérieurs que sont les ambassades.

C) L'observation participante : construction pluridisciplinaire d'un programme d'exercices cyber au CHU de Reims

Ma mission de stage professionnel visant à la construction puis mise en œuvre d'un programme d'exercices cyber à l'échelle du CHU de Reims débuta par la formation d'un groupe de travail pluridisciplinaire réunissant professionnels médicaux, paramédicaux et administratifs de l'établissement que je co-animais avec le RSSI et le référent paramédical des situations sanitaire exceptionnelles (SSE). Ce groupe fut l'occasion de questionner la connaissance du sujet par les équipes opérationnelles, les moyens disponibles et les besoins en exercice. De ces réunions (annexe 2) a pu rapidement éclore un kit homogène d'exercice cyber, adapté des ressources mises à disposition par l'Agence du numérique en santé (ANS).

D) Un travail de recherche nécessaire

Si le volet opérationnel pouvait essentiellement provenir des acteurs concernés explicitant leurs différents process de fonctionnement, les démarches stratégique et technique nécessitaient d'ores et déjà un travail de recherche documentaire, tant réglementaire qu'agrégeant les différents supports nationaux mis à disposition. J'entrepris ainsi la lecture de guides publiés par l'ANSSI et les kits mis à disposition par l'ANS. Je pris connaissance de la réglementation en vigueur et ses perspectives d'évolution. Le suivi de différents retours d'expérience fut également enrichissant aux fins d'anticiper les conséquences d'une cyberattaque. Liant rapidement le sujet cyber à la gestion de crise, je poursuivis mes recherches par l'appréhension des grands concepts sur ce sujet afin d'étayer ma réflexion institutionnelle.

E) Le choix d'une population cible à questionner

La fonction de responsable de la sécurité de systèmes d'information (RSSI) m'apparut comme une piste privilégiée de renseignement des outils disponibles et utilisés dans l'anticipation de la gestion de crise cyber. Massivement investie ces dernières années, cette fonction en établissement public de santé se trouve en effet au croisement des démarches stratégiques, techniques et opérationnelles.

F) Une première enquête menée par le biais d'un questionnaire électronique

Le questionnaire électronique fut diffusé auprès de DSI et RSSI sur le plan national (annexe 3). Il ne reçut pas un nombre de réponses satisfaisant pour constituer un échantillon représentatif mais il permit, par le vecteur de questions ouvertes, d'enrichir ma réflexion (annexe 4).

G) Des précisions nécessaires apportées par l'entretien semi-directif d'un groupe régional de RSSI

Cinq RSSI de GHT situés dans une région distincte de mon lieu de stage se sont rendus disponibles. Cette approche me permit, certes de les interroger au moyen d'une grille d'entretien semi-directif (annexe 5), mais aussi et surtout, d'enrichir mon travail de recherche au travers de leurs interactions.

Le sujet cyber demeurant sensible en établissement public de santé et afin de préserver l'anonymat des RSSI interrogés peu nombreux sur le plan national, aucun établissement support ni GHT ne sera cité dans le présent mémoire. Une exception est faite concernant l'établissement d'observation, lieu de stage professionnel facilement identifiable en usant des moyens numériques de communication.

1 Comprendre la crise ayant pour origine une cyberattaque afin d'anticiper ses conséquences : définitions, particularités et vecteurs de vulnérabilités en établissement public de santé

La compréhension des éléments composant une cyberattaque informatique apparaît comme un pré-requis à la construction de la démarche que nous pouvons mettre en œuvre pour anticiper ses conséquences. Il s'agit en effet de pouvoir la définir dans son environnement et son caractère polymorphe (1.1), pouvant être à l'origine d'une crise aux particularités notables (1.2). Enfin, il sera important d'étudier les évolutions numériques contemporaines susceptibles d'accroître la vulnérabilité des établissements publics de santé (1.3).

1.1 Définitions de la cyberattaque et ses particularités en établissement public de santé

1.1.1 De la création contemporaine d'une nouvelle dimension à l'exigence de cybersécurité

Il convient de rappeler en préambule de ce développement l'origine du préfixe *cyber,* décliné depuis la création du terme « cybernétique » employé pour la première fois en 1948 par Norbert Wiener, professeur au sein du Massachusetts Institute of Technology, dans son ouvrage « Cybernetics ». Visant initialement le « champ entier de la théorie de la commande et de la communication, tant dans la machine que dans l'animal » (Arpagian, 2022 :9), le préfixe « cyber » trouvera par la suite sa place dans la société de l'information née à la fin du XXème siècle.

A) Une nouvelle dimension : *cyberespace* et *datasphère*

L'appréhension de l'environnement dans lequel se meut cette forme de criminalité qu'est la cyberattaque nécessite alors de s'attarder sur la définition même du nouvel espace créé par les NTIC lui permettant de s'exercer. Nous le savons, les NTIC utilisent l'outil numérique que Dominique Vinck définit comme un « ensemble de procédés et techniques permettant de transformer n'importe quel objet en ensemble de données binaires » (Vinck, 2016 :9).

Cette définition renvoie ainsi au nombre et à la multitude de possibilités offerte par cet outil, créant une nouvelle dimension qu'est le *cyberespace*. L'ANSSI le définit alors comme un « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques » (Glossaire ANSSI, lettre C).

Dans ce nouvel espace transite un nombre exponentiel de données permettant d'utiliser le terme, lui aussi récent, de *datasphère*. Frédérick Douzet précisera d'ailleurs que cette dernière est « à la fois ancrée dans l'environnement physique, car elle repose sur une infrastructure physique et des acteurs économiques, mais aussi en grande partie indépendante du monde physique par sa fluidité et son ubiquité » (Douzet, 2020 :6). A partir de cette dernière définition, tout néophyte comprendra qu'en dépit d'une identification physique de stockage, d'alimentation et d'exploitation des données, ces dernières évoluent dans un environnement complexe, somme toute inatteignable sous certains aspects par l'être humain. L'acte de malveillance attaché à la cyberattaque réussira donc à s'introduire dans cet environnement multiforme échappant pour une partie aux personne chargées de l'exploiter dans la légalité.

Plus encore, nous pouvons convenir que la transversalité de la *datasphère* amplifie le phénomène d'une cyberattaque et que l'interconnexion mondiale du *cyberespace* est un terrain propice à l'augmentation de la fréquence des crises ayant pour origine une attaque cyber (Raimondo, 2022).

B) L'apparition de l'exigence de cybersécurité

La notion de cybersécurité s'est ainsi développée dans ce nouvel écosystème aux multiples enjeux. L'ANSSI la définit comme un « état recherché pour un système d'information lui permettant de résister à des évènements issus du *cyberespace* susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des serveurs connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense » (Glossaire ANSSI, lettre G).

La cybersécurité prend en compte l'ensemble des moyens techniques utilisés pour l'échange de données et pouvant faire « l'objet d'opérations d'infiltration, d'altération, de suspension, voire d'interruption » mais également « les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques » (Arpagian, 2022 :9-10).

Cette définition permet alors de visualiser une *cyberstructure* à protéger et composée, dans une approche simplifiée, de quatre couches :

- La couche physique renvoyant aux infrastructures, câbles, ordinateurs soumis aux contraintes de la géographie physique ;

- La couche logique visant les services assurant la transmission des données entre deux points du réseau (routage, nommage, adressage) ;
- La couche d'application permettant aux usagers d'accéder à Internet sans connaissance particulière de la programmation informatique. Des données sont alors régulièrement confiées par les usagers à ces applications ;
- La couche cognitive ou sémantique permettant l'information commune et l'interaction sociale (Douzet, 2014).

Plus encore, l'exigence de cybersécurité induit des mesures techniques et organisationnelles de sécurité préventives (contrôles d'accès, chiffrement des données, *etc*.), mais également des dispositifs de sécurité curatifs, se matérialisant en France par une obligation d'évaluation rapide des impacts de l'attaque activant le soutien d'autorités compétentes (ANS, ANSSI, CERT Santé). Cette dernière précision tenant à la mesure d'impact nous amène ainsi à envisager la polymorphie des cyberattaques.

1.1.2 De la variété apparente des cyberattaques au particularisme en établissements publics de santé : l'humain comme dénominateur commun

Il est intéressant de relever que l'ANSSI elle-même ne propose aucune définition de la cyberattaque dans son glossaire numérique, alors même que nous pouvons retrouver les notions de cybercriminalité, cyberdéfense ou de cybersécurité. Nous pourrions aussi user du terme de « cyberagression » ou encore de « vandalisme cybernétique ». Il s'agit en réalité d'autant de qualificatifs d'un acte malveillant envers un élément du *cyberespace*. Les variations de lexique témoignent finalement d'une grande polymorphie de cet acte malveillant, tout comme son degré de létalité.

A) <u>Les profils et motivations des cyberattaquants</u>

Dans un premier temps, nous pouvons aujourd'hui constater que les profils et motivations des cyberattaquants sont divers, la crise engendrée par la pandémie de Covid-19 ayant d'ailleurs mis en exergue cette pluralité des mobiles d'attaques. En effet, les premiers pirates informatiques des années 1980 recherchaient principalement la performance et le challenge en se confrontant à des équipes de recherche et développement aguerries. Il s'agissait en réalité de « prouesse technologique » (Arpagian, 2022 :17). Les années 2000 furent ensuite le théâtre de cyberattaques militantes permettant de conduire des « opérations d'influence pour […] mener des campagnes de mobilisation de l'opinion publique » (Arpagian, 2022 :17). Sans pouvoir affirmer que ces deux courants sont aujourd'hui révolus, nous pouvons convenir que la recherche de la rentabilité immédiate prend désormais le pas (Février, 2020). Ainsi, les possibilités d'extorquer des fonds ont été multipliées. Nous identifions le *phishing* (annexe 1) permettant d'usurper l'identité, notamment financière d'autrui ou encore le *ransomware* promettant la remise en

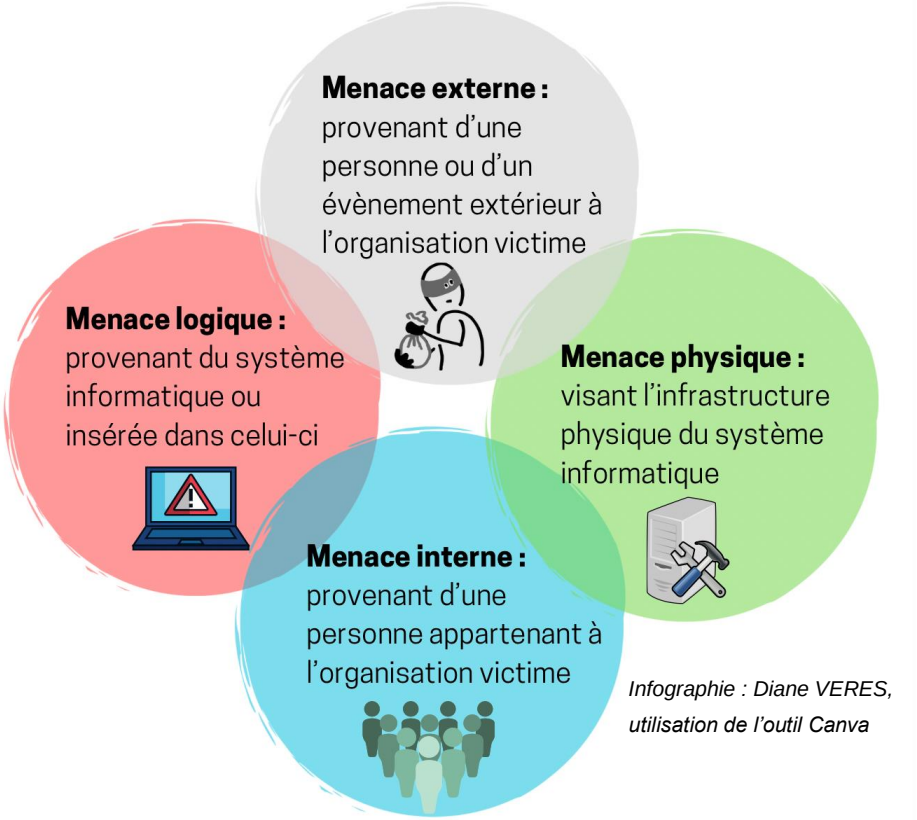
fonctionnement des systèmes d'information après paiement d'une somme d'argent. Mais la mise en danger de la e-réputation d'une entité est également source de rentabilité lorsque les représentations sociétales sont véhiculées par le *cyberespace*.

Une nouvelle motivation, tournée vers le secteur de la santé, est finalement apparue à l'occasion de la pandémie de COVID-19. En effet, si la proportion d'établissements de santé cyberattaqués était historiquement faible comparativement à d'autres organisations publiques ou au secteur marchand, elle fut exponentielle dès le début de cette période. Le contexte permettait de penser que l'attention portée à la lutte contre le virus doublée de la vulnérabilité des systèmes d'information de ces structures constituaient une porte d'entrée facilitée. Mais quel bénéfice en retirer face aux difficultés financières rencontrées par ces structures, à laquelle s'est ajoutée la recommandation ministérielle de ne pas répondre favorablement aux demandes de rançons ? Le premier, réside tout d'abord dans le ciblage de cette activité ayant continué à perdurer durant la pandémie, à l'inverse de nombreux autres secteurs freinés par la nécessité de protéger les populations (confinement, réduction des transports de marchandises, *etc*.). Le deuxième, souligné par l'ANSSI, relève de la lucrativité des données de santé, à même de compenser l'absence de rançon versée. Mais surtout, et conformément à un courant constant de motivations, la déstabilisation des institutions de santé à cette période permettait la déstabilisation d'un pays entier (Février, 2020).

Nous touchons alors à la motivation géopolitique historique des cyberattaquants. Le *projet GEODE* porté par l'Université Paris 8 met en lumière la prépondérance du facteur humain dans les motivations des cybercriminels par l'analyse géopolitique de la *datasphère*. Frédérick Douzet, prenant l'exemple de l'affaire *WikiLeaks* (piratage et publication des messages électroniques du parti démocrate américain), démontre que le succès de cette opération d'ingérence n'était pas tant la vulnérabilité des systèmes exploitants les registres électoraux et les machines à voter que la forte polarisation politique de la société américaine à cette époque (Douzet, 2020). Il confirme également l'importance pour les institutions étatiques d'investir cette nouvelle dimension. Une distinction s'est alors opérée entre pouvoir traditionnel étatique ou commercial et pouvoir distribué entre militants et internautes faisant du *cyberespace* le nouveau « terrain de la paix et de la sécurité collective » (Douzet, 2014 :14). La période de pandémie de COVID-19 ayant été nommée par le Président de la République française Emmanuel Macron comme une période de « guerre » (déclaration, 2020), nous pouvons aisément considérer que ce conflit s'est étendu au *cyberespace* dans lequel réside aujourd'hui des enjeux informationnels mais aussi organisationnels des établissements publics de santé.

B) Les menaces pesant sur les systèmes d'information et méthodologies employées par les cyberattaquants

Les menaces peuvent être identifiées selon quatre catégories, qu'elles résultent d'actes volontaires ou non :



Infographie : Diane VERES, utilisation de l'outil Canva

Conformément à cette infographie, nous pouvons rencontrer :

- Des menaces physiques externes renvoyant par exemple à des catastrophes naturelles (inondations, propagation d'un incendie extérieur, …) ou des actes de sabotage perpétrés par des personnes extérieures à l'organisation ;
- Des menaces physiques internes allant du simple fait de renverser une tasse de café sur un matériel informatique à l'incendie, volontaire ou non, d'une salle de serveur ;
- Des menaces logiques internes relevant d'un dysfonctionnement du système informatique d'origine interne ;
- Des menaces logiques externes relevant d'un dysfonctionnement du système informatique d'origine externe.

Il convient de relever le pourcentage désormais limité de risques liés à la menace physique, du fait notamment des nouvelles mesures de sécurité telles que les détecteurs de fumée permettant d'alerter précocement d'un départ de feu ou encore les badges d'accès empêchant les personnes extérieures à l'établissement de s'introduire dans les salles des serveurs aux fins de sabotage.

Les menaces logiques sont en revanche prépondérantes aujourd'hui et complexes à classifier selon la dualité menace interne / menace externe. En effet, pour le simple cas de la panne informatique, les établissements publics de santé sont confrontés à une menace interne lorsque la maintenance informatique relève de leur compétence comme à la menace externe lorsque cette action dépend d'un prestataire extérieur. Concernant les actes malveillants tels que la propagation de virus informatique, de *ransomware*, de *rootkit*, d'*advanced persistent threats*, de cheval de Troie ou encore de *keylogger* (annexe 1), la menace peut sembler principalement externe en raison d'une intention de nuire d'un cybercriminel, toutefois, la porte d'entrée est aujourd'hui majoritairement issue de la menace interne par la pratique du *phishing*.

Cédric Cartau mentionnera d'ailleurs que les « modes d'attaques de 2019 ne relèvent pas de l'attaque ciblée, mais plutôt de la pêche au filet […] Dès qu'une personne appartenant à une organisation publique ou privée a cliqué par erreur sur le lien ou la pièce jointe, le pirate a un pied dans la place et l'étape d'observation du réseau interne par le pirate commence. » (Cartau, 2019 :9). Partant de ce constat, nous pourrions affirmer que les cybercriminels usent désormais principalement de ce manque de sensibilisation des professionnels d'une entité et attendent que leur stratégie de *phishing* visant à extorquer des droits d'accès à un système d'information fonctionne. Autrement dit, la menace physique attire la menace logique.

Les établissements publics de santé n'échappent pas à ce constat. Aussi, le rapport public de l'OPSSIES fait-il mention d'une année 2022 marquée par un nombre important de vols d'identifiants de comptes de messagerie et d'accès à distance en indiquant comme mode opératoire des attaquants le *phishing*, l'exploitation des vulnérabilités sur des équipements qui n'ont pas été mis à jour et la technique de la force brute (annexe 1) visant à tester un grand nombre de mots de passe (OPSSIES, 2023).

Il convient de noter, selon ce même rapport, la diminution de 50% du nombre de signalements de *ransomwares* comparativement à l'année 2021 et pourtant prépondérants initialement en établissement de santé. Ce recours initial aux *ransomwares* est à mettre en regard avec les conséquences engendrées par ce type de cyberattaques : l'impossibilité d'accéder aux données générant possiblement une perte de chance pour le patient présent dans l'établissement de santé. La recommandation gouvernementale de non-paiement de la rançon a visiblement permis de détourner les attaquants de cette pratique.

Dès lors, dans les modalités d'attaques comme les conséquences motivant les cybercriminels, l'humain demeure le principal dénominateur commun.

1.2 Définitions de la crise et sa spécificité cyber en établissement public de santé

1.2.1 La définition complexe du concept de crise

Nous l'avons mentionné en introduction, toute cyberattaque ne sera pas nécessairement à l'origine d'une crise cyber. En témoignent par ailleurs les 58% de structures indiquant que l'incident n'a eu aucun impact sur leur organisation en 2022 (OPSSIES, 2023).

Dans son étymologie Krisis (grec) / Crisis (latin) signifie « décision ». Edgar Morin souligne qu'« aujourd'hui, crise signifie indécision. C'est le moment où, en même temps qu'une perturbation, surgissent les incertitudes » (Morin, 2012 :135). C'est alors à l'occasion de cette période d'incertitudes qu'il conviendra de trancher, de trier pour décider (Causse, 2013).

La crise souffre toutefois de l'implication de nombreux biais cognitifs ou non conscients pouvant complexifier son appréhension et, de fait, sa définition comme le démontrent les apports de Daniel Kahneman et Amos Tversky sur le sujet de la prise de décision face au risque. Décider en gestion de crise fait appel à des processus perceptifs (sensation), de reconnaissance mémorielle (mémoire) et de catégorisation (différenciation) auxquels peuvent aisément se mêler des biais de disponibilité (se contenter des premières informations disponibles), de confirmation (privilégier les informations confortant nos propres croyances et convictions) ou encore d'encrage (analyse d'un élément nouveau à l'unique lueur de sa compatibilité avec un schéma pré-établi).

L'absence de définition claire du concept de crise lui-même peut être constatée, renvoyant principalement la qualification de la crise à ses éléments de manifestations (Meszaros, De Coligny, 2015).

Pour qu'il y ait crise, Laurane Raimondo propose la réunion de quatre éléments cumulatifs observables :

- La rupture fondamentale de la continuité des activités usuelles ;
- La contrainte temporelle sensible de gestion ;
- L'omniprésence de l'ambiguïté, du moins en début de crise ;
- L'incertitude quant à la dynamique et la gravité de la situation (Raimondo, 2022).

Selon elle, le concept de crise peut également être appréhendé selon trois approches :

- L'approche par l'impact qui ne considère la crise qu'après son déclenchement eu égard aux conséquences observables du facteur déclenchant (nombre de victimes, ampleur d'une destruction, …) ;
- L'approche sectorielle considérant la crise comme le résultat de dysfonctionnements cumulés et potentiellement repérables. Une chaîne causale est alors établie sur le modèle du « fromage suisse » analysant les superpositions d'erreurs ;
- L'approche complexe mettant en avant la capacité de résilience d'une organisation en acceptant de vivre une crise tout en tirant partie de cette expérience (Raimondo, 2022).

Cette dernière approche dite « complexe » renvoie d'ailleurs à la théorie des *High Reliability Organization* (HRO) ou organisations à haute fiabilité initiée par Karlene Roberts. Ces HRO seraient ainsi capables de s'adapter à la complexité croissante de leur environnement et contenir les accidents rencontrés, sans chercher à les éviter.

Une analogie avec les établissements publics de santé français peut ainsi être soulevée. Alors que l'agilité et l'adaptabilité furent les maîtres mots de la gestion de crise COVID, force est de constater une certaine latence dans ce domaine. L'approche par l'impact ayant longtemps dominé, elle ne fut que tardivement complétée par l'approche sectorielle eu égard à d'autres domaines d'activités, notamment aéronautiques ou industriels. Pour exemple, la première analyse nationale des évènements associés aux soins en France fut réalisée en 2004, près de vingt années après l'affaire dite du « sang contaminé ».

Chacune de ces approches demeure cependant soumise à l'appréciation de la typologie de crise dans leur utilisation analytique. L'approche par l'impact permettra de porter une vision réactive sur la situation rencontrée tandis que l'approche sectorielle rationalisera ses causes. L'approche par l'impact ne donnera que peu voire pas d'outil d'anticipation de la crise alors que l'approche sectorielle présentera un biais de narration et, de fait, occultera le caractère imprévisible de la crise au risque de provoquer une sidération des acteurs non prévenus (Raimondo, 2022). Enfin, l'approche complexe permettant d'appréhender l'ensemble des composantes d'une crise peut à ce jour paraître fastidieuse, voire idéaliste et nécessite une adaptation au risque cyber, comme aux établissements publics de santé.

1.2.2 La particularité de la crise d'origine cyber en établissement public de santé

A) La particularité de la crise d'origine cyber

Selon l'ANSSI, la crise d'origine cyber revêt un caractère particulier par son essence même et comparativement à d'autres scénarios de crise en impliquant :

- « Une double temporalité avec des impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs semaines, voire plusieurs mois ;
- Une absence d'unicité de lieu de réalisation, qui sous-entend une potentielle propagation à d'autres organisations en raison de l'interconnexion des systèmes d'information ;
- Une menace s'adaptant aux mesures d'endiguement et de remédiation ;
- Une incertitude concernant le périmètre de la compromission ;
- Une complexité pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque » (ANSSI, 2021 :10-11).

La crise d'origine cyber est alors génératrice d'un ensemble de phénomènes cognitifs spécifiques. En effet, la peur de l'incompréhension peut amener les organes décisionnels à se reposer sur les seules expertises techniques et, de fait, limiter à une unique dimension un raisonnement par nature multifactoriel. En parallèle, face à une technicité accrue du sujet, la décision peut se fonder sur une vision simplifiée du système qui lui semble intelligible ou familière, au risque alors d'être inadaptée à la situation (Raimondo, 2022).

A ces phénomènes de quête de la rationalité se mêle la difficulté du *sensemaking*. Le besoin de créer du sens est important au regard de l'ambiguïté et de l'incertitude engendrées par toute crise, particulièrement dans l'environnement complexe du cyber. Aussi, Laurane Raimondo identifie-t-elle six étapes de raisonnement au sein des cellules de crise, exacerbant certains biais cognitifs :

- L'ambiguïté créée par le manque de compréhension du sujet des décideurs ;
- L'interaction amenant les acteurs à se forger une représentation de la situation ;
- La réification visant l'interprétation globale cohérente admise par une compréhension collective des éléments ;
- La communication permettant l'adoption commune des actions à mettre en œuvre ;
- La plausibilité aidant à simplifier la représentation du réel pour éviter les incohérences ;
- Le bricolage renvoyant à l'idée qu'une équipe peut utiliser les éléments mobilisés de manière inédite pour répondre à l'évènement (Raimondo, 2022).

B) Son application aux établissements publics de santé

Dans sa déclaration du 18 février 2021 portant sur les cyberattaques dans les hôpitaux et la stratégie nationale pour la cybersécurité, Monsieur le Président de la République Emmanuel Macron mentionnait que nous avions pu voir « à quel point ces attaques cyber qui peuvent paraître abstraites, et c'est vrai qui ne faisaient pas partie du quotidien de notre pays et dont on parlait peu, peuvent en quelques instants venir percuter tout un système d'organisation […]. Tout cela montre bien combien cette menace est extrêmement sérieuse, parfois vitale » (déclaration 2021). Ainsi, l'indisponibilité du numérique en établissement public de santé aurait la possibilité de percuter le fonctionnement global de l'entité. Mais comment ?

Tout d'abord car sans outil numérique, la communication se complexifie dans une organisation hospitalière nécessitant nombre d'appels téléphoniques et d'échanges de courriels pour assurer la fluidité du parcours du patient. Il ressort en effet des nombreux échanges avec les acteurs opérationnels du CHU de Reims une réelle inquiétude quant à une possible indisponibilité de leurs outils téléphoniques.

Ensuite car la gestion administrative elle-même repose sur le numérique, nous pouvons penser au dossier patient informatisé (DPI) comme au système médico-tarifaire du programme de médicalisation des systèmes d'information (PMSI). Aussi, en cas d'indisponibilité de l'outil numérique, les équipes soignantes s'exposent-elles à l'impossibilité d'accéder aux données du patient, mais également de valoriser leur activité.

Mais la dépendance d'un établissement public de santé à ses services numériques va plus loin aujourd'hui, comme en témoigne le développement des systèmes de supervision connectés (automates de préparation, transports automatisés lourds, ascenseurs, *etc*) mais aussi le recours à l'intelligence artificielle permettant l'atteinte d'une nouvelle technicité médicale.

Sans disponibilité du numérique, toutes ces activités subissent un coup d'arrêt, brutal. Nous entrons alors dans la définition de la crise d'origine cyber donnée par l'ANSSI : « la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, *etc*.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques [auxquels sont associés les systèmes d'information de l'organisation et ceux de ses prestataires] (cyberattaques de type rançongiciel, déni de service, *etc*.). C'est donc un événement à fort impact, qui ne saurait être traité par les

processus habituels et dans le cadre du fonctionnement normal de l'organisation » (ANSSI, 2021 :10).

En soulignant la nécessité « d'une ou plusieurs actions malveillantes », l'ANSSI exclut dès lors les événements accidentels. Pour autant, la frontière peut, en pratique, paraître poreuse entre les différents types d'indisponibilité des services numériques. Nous devons alors prendre en compte le niveau d'incertitude engendré par une action malveillante qui sera fonction du périmètre de la compromission afin de caractériser ou non la crise. L'ANSSI précise également que les actions malveillantes n'entraînant pas l'interruption immédiate et majeure des services essentiels de l'organisation sont exclues de la définition de la crise d'origine cyber.

Ces éléments complémentaires nous permettent donc d'éclairer le chiffre précédemment évoqué de 58% de structures indiquant que l'incident n'a eu aucun impact sur leur organisation en 2022. Cependant, 63% des structures indiquaient que l'incident avait eu un impact sur les données (OPSSIES, 2023). Or, la fuite de données, particulièrement à caractère personnel, demeure un enjeu majeur de la gestion de crise d'origine cyber des derniers mois. Rappelons ainsi l'effroi provoqué chez 1,4 millions de français lors du vol, par piratage informatique et confirmé par l'Assistance publique-Hôpitaux de Paris, de données confidentielles collectées à l'occasion des tests Covid réalisés durant l'été 2020. Pour autant, la définition restrictive éditée par l'ANSSI permet de recentrer la notion de crise d'origine cyber autour du risque principal de perte de chance pour le patient en raison d'une déstabilisation immédiate et majeure du fonctionnement de l'organisation. C'est bel et bien l'anticipation de ce risque premier qu'il conviendra de souligner et faisant la spécificité du risque cyber en établissement public de santé.

1.3 La numérisation des établissements publics de santé comme vecteur de vulnérabilités

1.3.1 Des transformations numériques nationales impliquant les établissements publics de santé

Monsieur le Président de la République Emmanuel Macron précisait également dans son discours du 18 février 2021 suscité que : « le paradoxe, c'est qu'au moment où la menace devient tangible et visible, c'est aussi le moment où nous devons accélérer sur la numérisation de beaucoup de choses » (déclaration, 2021). En effet, alors que nous venons de démontrer la vulnérabilité certaine des établissements publics de santé face à une paralysie de leurs systèmes d'information, ces derniers sont engagés à davantage numériser leurs activités par les orientations publiques nationales.

A) La dématérialisation multiplicatrice des portes d'entrée dans les systèmes d'information

Considérée comme un vecteur de simplification de l'action publique, la dématérialisation s'est progressivement imposée dans les administrations françaises. Initiée depuis quelques années, notamment en matière de marchés publics afin de s'aligner sur nos voisins européens, la dématérialisation entre dans le nouveau tournant de « l'Objectif 0 papier » réaffirmé en 2021 par le cinquième Comité interministériel de la Transformation Publique et l'édition d'un guide assorti de fiches outils et méthodologiques. Littéralement, la dématérialisation renvoie à la suppression du support matériel. Dès lors, et dans une acception large, cette dernière vise à numériser l'ensemble des classeurs, cahiers, parapheurs ou encore feuilles volantes des agents publics. Ce phénomène n'est d'ailleurs pas récent si nous nous référons aux bases de données internes numériques mises en place dès les années 1980, suivies de la possibilité de transporter ses documents de travail dans de petites clés USB pour aboutir aujourd'hui à un accès à l'ensemble des serveurs de notre organisation à distance (depuis son domicile ou ailleurs). Cette évolution permet ainsi une réalisation de son exercice professionnel en télétravail.

Le décret n°2016-151 du 11 février 2016 fut ainsi le premier texte réglementaire à instaurer les conditions et modalités de mise en œuvre du télétravail dans la fonction publique. La pandémie de COVID-19 a ensuite marqué un tournant dans cette pratique professionnelle dont le cadre a été reposé par l'ordonnance n°2021-1574 du 24 novembre 2021, codifié à l'article L.430-1 du Code de la fonction publique et harmonisé par l'accord relatif à la mise en œuvre du télétravail dans la fonction publique rendu public le 3 avril 2022. Cette période pandémique et d'expansion du télétravail peut alors être corrélée à l'augmentation du nombre de cyberattaques comme en témoignent les nombreux appels à la vigilance émanant des organismes officiels durant cette période (annexe 6). Le récent accord susscité précise d'ailleurs que « tous les lieux d'exercice du télétravail doivent respecter les conditions de sécurité et de confidentialité » et que « l'employeur reste responsable de la sécurité des données personnelles traitées par les agents à titre professionnel » (accord 3 avril 2022). Ces précisions mettent en lumière l'amplification de la menace logique par une moindre sécurisation de la connexion internet par exemple mais aussi de la menace physique au regard du risque important de perte ou de vol du matériel informatique nomade en dehors des locaux.

B) La e-administration vectrice des campagnes de *phishing*

Parallèlement à cette dématérialisation modifiant les organisations de travail s'est également installée la nécessité de transformer numériquement l'accès aux administrations françaises. Initiée dès le début du XXIème siècle avec le programme d'action gouvernemental pour la société de l'information (PAGSI) afin de faciliter la diffusion en ligne des informations publiques, cette numérisation de l'administration débouchera rapidement sur la naissance des téléprocédures visant à réaliser, à distance et par le vecteur de l'Internet, les démarches administratives sur le territoire. Cette évolution acte, en 2016, le déploiement d'une identité nationale numérique permettant d'accéder, via l'outil *France Connect*, à la quasi-totalité des administrations en ligne. Cette identité numérique contient ainsi les informations personnelles nécessaires aux citoyens afin de réaliser en ligne leurs démarches fiscales, de sécurité sociale, d'immatriculation ou encore de formation.

La prise de contrôle sur cette identité apparaît alors comme une aubaine pour les cyberattaquants au regard des informations qu'elle recouvre. Plus encore, la nécessité grandissante de réaliser nos démarches administratives sans recours physique possible alimente la crédulité des citoyens lorsque les cyberattaquants engagent à leur encontre une campagne de *phishing* (Février, 2020). Toute personne dotée d'un moyen de communication numérique ou téléphonique a pu faire l'objet d'un e-mail ou SMS l'informant qu'une somme était à payer au titre d'une amende ou encore que leur compte professionnel de formation nécessitait leur attention. Ces campagnes de *phishing* permettent ainsi au cyberattaquant de se saisir de l'identité numérique de la personne hameçonnée et, en sus de l'accès à ses données personnelles, modifier les coordonnées bancaires et détourner certains financements disponibles comme, par exemple, des prestations de sécurité sociale.

C) Le numérique en santé ou le difficile équilibre à trouver sur le traitement des données de santé

Mise en place par l'arrêté du 29 novembre 2019 et accompagnée d'un plan stratégique 2019-2022, la plateforme nationale des données de santé ou *Health Data Hub* est un groupement d'intérêt public visant à « réunir, organiser et mettre à disposition les données […] de santé et de promouvoir l'innovation dans l'utilisation des données de santé » (loi n°2019-774 du 24 juillet 2019). Créée à la demande de Monsieur le Président de la République Emmanuel Macron afin de rattraper le retard de la France en matière de traitement des données de santé et d'innovation dans le domaine, son hébergement et ses logiciels de traitement ont été confiés à l'entreprise Microsoft, soulevant de nombreux questionnements quant à la sécurité de ces données. Pourquoi ? Principalement en raison de la non-conformité au RGPD du choix de ce prestataire autorisé par la loi fédérale

américaine à transmettre des informations sans consentement préalable aux forces de l'ordre et agences de renseignements américaines. Une lutte juridique s'en est d'ailleurs suivie entre exigences européennes et conciliation française aboutissant à une nécessaire mutation de cet hébergement vers une solution européenne, voire nationale plus sécurisée dans les prochaines années. Mais cette plateforme nationale des données de santé se veut également être un guichet unique permettant leur consultation ainsi qu'un réseau à même de mettre en relation les différents acteurs de l'écosystème. Le secteur de la santé se trouve ainsi tiraillé entre innovation et protection de données susceptibles d'attirer nombre de cyberattaquants compte tenu de leur nature en matière de santé : informations administratives relatives à la personne physique, informations obtenues lors de tests ou examens d'une partie du corps ou d'une substance corporelle et informations d'anamnèse (maladie, handicap, traitement clinique, antécédents médicaux, *etc*.).

Parallèlement, la France est également entrée durant l'année 2019 dans une nouvelle dynamique de développement de la e-santé. Elle résultait d'un constat alarmant soulevé par le rapport « Accélérer le virage numérique » de Monsieur Dominique Pon et Madame Annelore Coury en 2019 mettant en exergue le retard français en matière de coordination des professionnels de santé par l'outil numérique et le renforcement de la place de l'usager dans cette nouvelle dimension. La première feuille de route du numérique en santé fut ainsi éditée pour la période 2019-2022 en se donnant l'objectif d'un numérique « incarné par des humains, au service de l'humain » (Ministère de la santé, 2019 :4). La création de l'espace numérique de santé au service des patients et des professionnels en constitua alors la mesure phare en permettant des échanges documentaires dématérialisés entre ces acteurs. Lui succède depuis le 17 mai 2023 une édition pour la période 2023-2027 visant à « mettre le numérique au service de la santé » et souhaitant poursuivre l'investissement de cet outil considéré comme un axe majeur de la transformation du système de santé français. Pour autant, et dans la continuité des anciennes défiances adressées envers le Dossier Médical Partagé (DMP), de nombreuses inquiétudes persistent quant à la sécurisation de ces données transitant dans le *cyberespace* et la motivation qu'elles peuvent induire pour les cyberattaquants. Nous l'avons vu, la déstabilisation est un mobile fort des cyberattaques et les données de santé recouvrent une importance primordiale pour les populations. Leur vol engendre donc une perte de confiance non négligeable envers les autorités publiques ayant instauré ces nouveaux flux d'échanges. Pour autant, le développement numérique du secteur de la santé apparaît comme une piste privilégiée d'amélioration du parcours du patient dont la nécessité se retrouve au sein même de l'environnement territorial des établissements publics de santé.

1.3.2 Des nécessités territoriales et internes obligeant les établissements publics de santé

A) L'interopérabilité des logiciels métiers et le risque de réactions en chaîne

L'impératif de partage des données de santé entre acteurs du système engage alors les établissements publics de santé à œuvrer à l'interopérabilité des logiciels avec ces nouveaux outils ou, autrement dit, de permettre aux logiciels métiers internes à une structure de fonctionner avec d'autres produits ou systèmes d'information. Nous pouvons prendre comme exemple la mise à disposition dans l'espace numérique de santé des patients des lettres de sortie d'hospitalisation contenues dans le dossier patient informatisé (DPI) de l'établissement public de santé. Ce processus de recueil du document nécessite alors une mise en compatibilité du DPI avec la brique de l'espace numérique de santé permettant de le mettre à disposition de l'usager.

Mais l'interopérabilité des logiciels au sein des établissements publics de santé peut également se retrouver dans le report de données d'un appareil connecté à un autre logiciel du système d'information. Ici encore, il s'agit bien de flux de données entre logiciels différents certes, mais également entre entités différentes. En effet, les établissements publics de santé ont recours à de nombreux prestataires à même de leur fournir les solutions technologiques nécessaires à leur activité. Or, nous pouvons aisément convenir que l'infection d'une brique interopérable et, de fait, connectée avec d'autres, mènera à une réaction en chaîne de contamination.

B) La convergence des systèmes d'information dans les groupements hospitaliers de territoire soulevant la difficile question des accès

Les établissements publics de santé sont ainsi enjoints depuis plusieurs années à développer les vecteurs d'échanges des données de santé entre acteurs et particulièrement au sein de leur territoire. Il convient de rappeler que la mise en œuvre des GHT par la loi n°2016-41 du 26 janvier 2016 a investi les établissements supports de « la stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier (SIH) convergent, en particulier la mise en place d'un dossier patient permettant une prise en charge coordonnée des patients au sein des établissements parties au groupement » (art. 107 de la loi n°2016-41).

Ainsi, le guide produit par la DGOS en juillet 2016 propose quatre modèles de convergence des systèmes d'information :

- La coopération : partage des données statistiques via les outils de réseau (DMP, messagerie sécurisée, réseaux d'imagerie régionale) ;

- La fédération : les établissements du GHT partagent des données statistiques dans un réceptacle commun sur la base d'un serveur de rapprochement d'identité territorial ;
- L'intégration : les établissements du GHT, pour certains ou sur une partie du SIH, mettent en œuvre des agrégats homogènes ;
- L'unification : les établissements du GHT choisissent de mettre en œuvre un même DPI accompagné d'un référentiel d'identités unique, permettant un suivi des parcours de soins dans un seul et même outil (DGOS, 2016).

L'unification doit ici être appréhendée comme la finalité de l'obligation légale de convergence des systèmes d'information au sein d'un GHT afin de fluidifier les parcours des usagers. Mais, alors que chaque établissement disposait initialement de son propre DPI aux accès et infrastructures de stockage strictement internes et locaux, le paradigme est inversé en ouvrant un DPI au niveau territorial, augmentant le nombre de personnes autorisées à y accéder et ce, depuis des infrastructures différentes sur le territoire. Nous pouvons ainsi aisément imaginer que l'attaque d'une seule infrastructure permet de déstabiliser l'ensemble des établissements parties à un GHT.

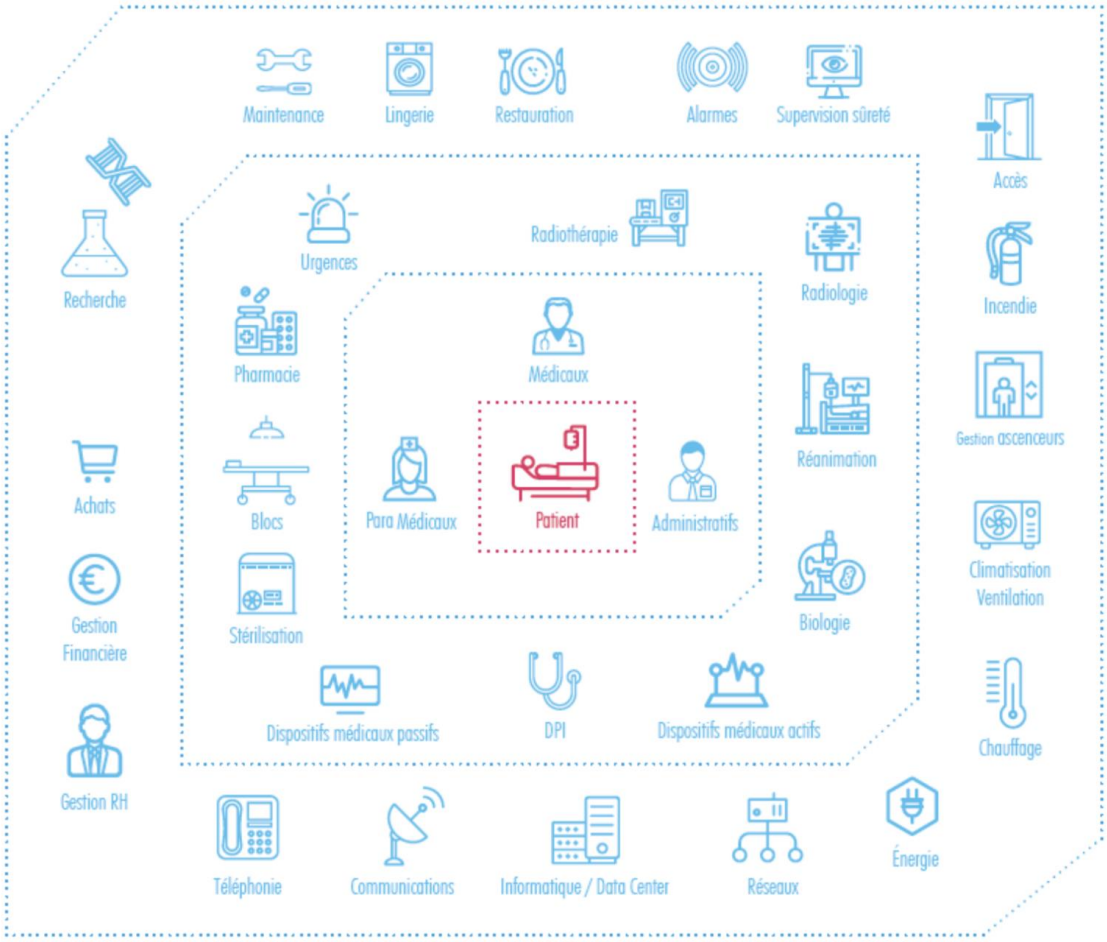
C) L'établissement public hébergeur de données de santé : une responsabilité croissante des établissements parties à un groupement hospitalier de territoire

Dans le cadre de la convergence des SIH instaurée à l'échelle d'un GHT, l'établissement support peut aisément se trouver dans la position d'un hébergeur des données de santé (HDS) considéré, par l'article L.1111-8 du Code de la santé publique comme « toute personne qui héberge des données de santé à caractère personnel […] pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ». Un référentiel attaché à une certification HDS est ainsi rendu opposable. Pour autant, la doctrine du numérique en santé, de même qu'une interprétation réalisée par le ministère chargé de la santé publiée sur le site de l'ANS le 15 décembre 2022, précise qu'un établissement de santé peut être exempté de la certification HDS à la condition du respect de 3 éléments cumulatifs :

- La convention constitutive du GHT prévoit explicitement la délégation d'activité d'hébergement à l'établissement concerné. Cette mention a pour effet d'instaurer une co-responsabilité de traitement au sens du RGPD ;
- Un accord de co-responsabilité de traitement est conclu entre l'ensemble des établissements parties au GHT afin de permettre l'engagement de responsabilité de l'ensemble des établissements en cas de manquements aux dispositions du RGPD ;

- Des mesures doivent être prises pour assurer la sécurité et la confidentialité des données hébergées. Le niveau exigé est défini dans le cadre d'un dispositif de certification SI (ISO 27001 par exemple).

Nous constatons dès lors la prégnance du respect du RGPD et des responsabilités attachées permettant de protéger les données de santé. Elle témoigne d'une menace s'intensifiant avec cette ouverture des systèmes d'information au service de l'usager et qu'il convient désormais d'anticiper.



Ministère des solidarités et de la santé, ANS – Campagne nationale d'information sur la cybersécurité en santé – Dossier d'information – Mai 2021

2 Les outils d'anticipation de la crise d'origine cyber : entre pistes nationales et culture d'établissement

L'étude des définitions entourant la notion de crise d'origine cyber et des enjeux contemporains des établissements publics de santé pouvant être facteurs de vulnérabilité nous ont ainsi permis d'appréhender l'importance du risque cyber. Il convient désormais de s'intéresser aux outils pouvant actuellement être mobilisés afin d'anticiper les conséquences d'une attaque cyber dans un objectif de résilience. La démarche à structurer sera ainsi abordée dans un premier temps (2.1) permettant d'engager un travail de réflexion sur la production documentaire nécessaire à l'anticipation de la survenue du risque (2.2) mais également d'investir sa nécessaire sensibilisation et simulation (2.3).

2.1 Des démarches à structurer et à lier

La démarche d'anticipation du risque cyber s'instaure alors comme un pré-requis de réussite. Impliquant diverses directions fonctionnelles de l'établissement public de santé, cette démarche sera ainsi à construire stratégiquement au niveau de la gouvernance (2.1.1). Sa matérialisation devra également être technique en raison de l'essence même du sujet traité (2.1.2). Enfin, le volet opérationnel, en qualité de principale victime d'une crise cyber devra être investi afin, nous le rappelons ici, d'éviter toute perte de chance pour l'usager du système de santé (2.1.3).

2.1.1 Une gouvernance équilibrée de la démarche : l'enjeu de la polymorphie fonctionnelle

A) <u>Les acteurs concernés</u>

Il ressort tout d'abord des différents entretiens menés la nécessité d'une prise de conscience institutionnelle de l'enjeu cyber au sein d'un établissement public de santé. En effet, le positionnement du chef d'établissement en faveur de la démarche d'anticipation apparaît comme un prérequis essentiel à l'investissement futur de l'ensemble de la structure. Conformément à l'article L.6143-7 du Code de la santé publique, le chef d'établissement « conduit la politique générale de l'établissement ». Plus encore, l'arrêté du 13 décembre 2016 le désigne expressément comme autorité qualifiée pour la sécurité des systèmes d'information (AQSSI). Il est à ce titre responsable de la sécurité des systèmes d'information de sa structure et s'assure de « l'application des instructions ministérielles données en cette matière ».

L'ensemble des directions fonctionnelles seront également amenées à réfléchir aux outils d'anticipation propres à leurs missions et fonctionnements. Pour autant, les directions liées aux Systèmes d'Information (DSI), à la Qualité et Gestion des Risques et à la Communication seront également investies d'une mission transversale, aussi bien stratégique qu'opérationnelle dans l'anticipation de la crise d'origine cyber.

La gouvernance de la démarche ne peut pour autant se réduire à l'équipe de direction. Aussi, le président de CME ainsi que les différents chefs de pôles et cadres supérieurs de pôles seront des piliers importants et structurants à mobiliser dans le cadre de la gouvernance de la démarche.

Enfin, le RSSI pourra se faire le pivot de la traduction technique, opérationnelle mais également stratégique par les missions qui lui sont confiées en vertu de sa désignation par l'AQSSI. Les récents référentiels (MATURIN'H, SUN-ES notamment) renforcent d'ailleurs son positionnement stratégique en prévoyant que ce dernier est en charge de promouvoir et accompagner les bons usages et les pratiques de sécurisation au quotidien au sein des services de soins. Cette dimension inclut dès lors la sensibilisation à la prévention des risques numériques auprès des différents acteurs de l'établissement. Le Guide d'aide à la préparation du plan blanc numérique en établissement de santé le qualifie même d'« interlocuteur privilégié du personnel et de la direction de l'établissement sur la sécurité des systèmes d'information […]. Il facilite la remontée des informations concernant la réalité du terrain. Le RSSI rend compte a minima semestriellement à la gouvernance de l'établissement de l'évolution des risques numériques et des avancées dans la mise en conformité du système d'information » (DGOS, 2023 :6).

B) La structuration de la démarche

La structuration de la démarche dépendra de l'organisation et de la culture internes à l'établissement public de santé. Pour autant, nous pouvons avancer ici certaines pistes de réflexion issues de la consultation simultanée de cinq RSSI.

La démarche doit tout d'abord être unanimement tournée vers l'acculturation et la prévision des éléments à mobiliser le jour de la survenue d'une cyberattaque. Il conviendra de prévoir une matérialisation de la démarche dans une optique de construction certes mais usant ensuite de l'analyse et de l'amélioration continue. Autrement dit, cette démarche ne doit pas avoir pour seul objectif d'éditer de la documentation, il faut aussi la faire vivre et lui permettre de s'adapter aux diverses évolutions, particulièrement nombreuses dans l'environnement cyber.

En raison de la transversalité des actions nécessaires à l'anticipation du risque cyber, des instances de suivi de la démarche doivent être mises en place. Leur constitution dépendra toutefois de la culture de l'établissement. Lors de mon entretien mené avec les RSSI, chacun avait une approche différente des instances de concertation de gouvernance de la démarche : comité de pilotage (COPIL) d'établissement dédié au sujet ; réunions mensuelles de coordination réunissant le chef d'établissement, la DSI et la Direction des finances ; COPIL situations sanitaires exceptionnelles, *etc*. Il s'agit dès lors pour l'établissement public de santé de trouver ou créer ce temps d'échange formalisé dédié à la démarche et à son suivi.

La structuration stratégique de la démarche devra également prendre en compte la dimension GHT dans le contexte de convergence des SIH. Cependant, il convient de préciser que si les RSSI interrogés avaient pu l'intégrer dans leurs réflexions, en envisageant notamment le risque cyber au sein de leur schéma directeur des systèmes d'information (SDSI) GHT et l'abordant à l'occasion de réunions dédiées au GHT, la mise en œuvre des actions reste variable d'un établissement partie à l'autre. Ce constat résultant d'un échantillon de RSSI de GHT doit également être corrélé à la nomination tardive d'un « RSSI de GHT » dans le cadre de la convergence des SIH. Aussi, 68% des GHT répondants avaient officiellement nommé un RSSI pour le GHT en 2020. Ils n'étaient que 26% en 2018 (Atlas des SIH, 2020). Un certain retard accentué par la pandémie de COVID-19 peut donc être avancé dans cette sécurité convergente des SI. Nous pouvons également souligner la difficulté des RSSI à disposer de relais stratégiques et techniques dans les établissements parties au GHT.

2.1.2 Une structuration de la technique, gage de son institutionnalisation

A) <u>L'investissement national des DSI</u>

Nous constatons ainsi que, si les agents des DSI ont longtemps été circonscrits à la mission de maintenance des infrastructures et de recherche de solutions logicielles pour les Métiers, les cartes sont aujourd'hui considérablement rebattues en présence du risque cyber croissant.

Comme le souligne Rémy FEVRIER, « la DSI ne peut plus être uniquement considérée comme une fonction support : elle devient aussi stratégique que la DAF ou la R&D » (Février, 2020 :90). L'obligation de désigner un RSSI ainsi qu'un délégué à la protection des données majoritairement rattachés à la DSI dans les établissements publics de santé en témoigne. Plus encore, la dimension stratégique de la DSI est aujourd'hui appuyée par de nombreuses recommandations nationales, notamment le récent Guide d'aide à la préparation d'un plan blanc numérique publié au Journal officiel le 30 juin 2023. Ce dernier

agrège en effet les différents prérequis nécessaires à l'anticipation du risque cyber et parmi eux la nécessité d'impliquer le « service en charge des systèmes d'information ».

Cette implication demandée recouvre alors différents volets, allant de la collaboration avec les Métiers à la sécurisation technique des infrastructures. La démarche technique doit par ailleurs progressivement s'imprégner de la démarche qualité en s'intéressant à l'analyse des risques potentiels pesant sur son système d'information. Elle gagne ainsi en transversalité. La visée stratégique est d'autant plus prégnante dans les 135 établissements supports de GHT disposant du statut d'OSE soumis à la déclaration d'un point de contact auprès de l'ANSSI mais également de leurs systèmes d'information essentiels (SIE) et l'application de règles de sécurité nationalement définies à ces derniers.

Comme évoqué précédemment, les référentiels nationaux auxquels les DSI doivent répondre s'accumulent. Vient également se greffer une politique générale de sécurité des systèmes d'information en santé (PGSSI-S) à laquelle chaque DSI doit se conformer dans la rédaction de sa politique locale de sécurité des systèmes d'information (PSSI). La DSI acquiert dès lors un rôle stratégique en produisant une politique transversale, dépassant le schéma directeur des systèmes d'information. Elle est en effet amenée à développer des principes techniques mais également organisationnels et de mise en œuvre.

B) L'investissement local des DSI

Afin de parvenir à une institutionnalisation de la démarche technique de sécurité des systèmes d'information, la DSI devra adopter une posture de simplification des éléments techniques en adaptant son discours aux interlocuteurs rencontrés, à commencer par le chef d'établissement.

Son action, en matière d'anticipation du risque cyber recouvre tout d'abord un aspect purement informatique visant à éviter que le système s'arrête. Il s'agira alors de l'ensemble des moyens dédiés à la sécurisation des systèmes (accès, mise à jour, chiffrement des données, *etc*.). Mais la DSI devra également anticiper les moyens permettant de limiter le caractère invalidant de l'arrêt du système (mise à disposition de sauvegardes, réduction du temps de résolution de l'incident). L'aspect technique portera davantage sur l'investissement porté à l'infrastructure. Il s'agira par exemple de doubler les composants ou de permettre une deuxième sauvegarde sur un site extérieur. Enfin, l'aspect organisationnel de l'anticipation doit permettre à chaque technicien de connaître la marche à suivre en cas de cyberattaque avérée. Ce dernier volet nécessite donc d'investir au sein de la DSI des instances de vigilance, d'arbitrage et de pilotage pouvant rendre compte de leur activité à l'AQSSI. Il convient également de garder à l'esprit qu'à la survenue d'une

cyberattaque, la DSI sera particulièrement sollicitée par les autorités compétentes averties en vertu de l'article L.1111-8-2 du Code de la santé publique. Elle devra être à même de fournir dans des délais restreints l'ensemble des éléments nécessaires à une résolution rapide et à la limitation des conséquences invalidantes de l'incident. Et cela se prépare également, stratégiquement.

2.1.3 Le cadrage opérationnel : pré-requis d'une adéquation de la démarche aux particularités locales

A) Les Métiers comme victimes directes d'une cyberattaque

Comme étudié, les Métiers composant l'établissement public de santé seront les victimes directes d'une interruption des systèmes d'information en cas de cyberattaque, au risque de mettre en péril la prise en charge du patient. Un cadrage mêlant stratégie, technique et opérationnalité est alors indispensable à l'anticipation du risque cyber. Comme l'abordent Stéphanie Chauvin et Jean-Baptiste Igonetti, la performance organisationnelle repose sur du capital humain, du capital savoir et du capital organisationnel (Chauvin, Igonetti, 2020). Ainsi, les Métiers devront être sensibilisés à une potentielle crise d'origine cyber, connaître les réflexes nécessaires, et mettre en œuvre une organisation qualifiée de « mode numérique dégradé ». La Technique aura également besoin de s'enquérir des besoins que pourront exprimer les Métiers ; tant en matière de sécurisation préalable que d'adaptabilité du niveau de réponse à une cyberattaque.

L'enrichissement de ces trois capitaux ne peut alors reposer sur une logique purement descendante et nécessitera une co-construction de la démarche organisationnelle. Nous retrouverons ainsi les compétences informatiques pour fournir des solutions informationnelles relevant du « mode numérique dégradé » (PC de remédiation, clés 4G, impressions des sauvegardes, *etc*.), mais également des compétences de qualité et de sécurité des soins afin d'organiser le fonctionnement même du service opérationnel en « mode dégradé » (procédure, dossiers papiers, garanties de l'identitovigilance, *etc.*).

Il convient de préciser que les directions fonctionnelles sont elles aussi susceptibles d'être considérées comme des victimes directes d'une cyberattaque lorsqu'elles se trouvent en position de Métiers vis-à-vis de l'outil informatique. Nous pouvons ainsi penser à l'indisponibilité des logiciels de paie impactant les directions des ressources humaines (paramédicales et médicales) ou de supervision des équipements, comme la température de locaux de stockage, dont le suivi relève d'agents de directions de services supports.

B) La nécessité d'identifier un coordonnateur de la démarche opérationnelle

Dès lors, les directions fonctionnelles seront impliquées, tant en qualité d'organes de gouvernance que de Métiers pouvant être déstabilisés à la suite d'une cyberattaque rendant indisponible l'accès aux systèmes d'information. Ce positionnement, conjugué au nombre important de services opérationnels à accompagner, nécessite alors l'identification d'un coordonnateur à même d'organiser et de piloter la démarche opérationnelle d'anticipation d'une cyberattaque. Nous en conviendrons, aucune exigence technique ne peut être imposée à ce dernier. Le profil recherché résiderait plutôt dans une capacité organisationnelle, un intérêt pour le sujet mais aussi une disponibilité transversale. Les RSSI interrogés n'ont ainsi fait aucune proposition de poste formellement identifié. Pour certains établissements, ce coordonnateur était un référent SSE, pour d'autres un RSSI ou encore conjointement les directeurs des systèmes d'information et de la qualité. Il s'agit en réalité de choix principalement personnel-dépendant.

Le niveau d'action de ce coordonnateur est également à définir. Compte tenu des différents échanges sur le sujet, nous pourrions lui accorder une mission de supervision de la communication puis d'avancement de la démarche dans les services. Il peut, pour cela, disposer de relai au sein des pôles d'activités selon le niveau de délégation choisi par la gouvernance et pouvoir reposer sur des éléments tangibles du niveau de préparation des équipes au risque cyber.

Aussi, mon stage professionnel au CHU de Reims a été l'occasion de réfléchir à l'édition d'un tableau de bord permettant de suivre l'avancement de cette démarche opérationnelle. Il convenait alors de recenser, à l'aide d'un tableur *Excel*, l'ensemble des unités fonctionnelles du Centre hospitalier universitaire (CHU) en abscisse afin d'y adjoindre en ordonnée les différents points d'avancement de chacun dans la démarche :

1) Pourcentage des effectifs ayant bénéficié d'une action de formation ou de sensibilisation au risque cyber ainsi que la date de recensement ;
2) Existence d'un plan de continuité d'activité (PCA) et/ou plan de reprise d'activité (PRA) pour le service ;
3) Liste des procédures « mode numérique dégradé » en lien avec le risque cyber ;
4) Réalisation d'exercices, dates afférentes et améliorations envisagées à l'occasion de chacun d'eux.

Si les actions de formation et de sensibilisation ainsi qu'une liste de procédures « mode numérique dégradé » demeurent indispensables, l'ensemble des autres rubriques proposent un item « sans utilité ».

En détention de cet outil, le coordonnateur de la démarche ne peut être nécessairement en charge de s'enquérir des informations personnellement. Ainsi, une trame de positionnement a été éditée afin qu'un encadrement de proximité puisse se faire le relai de la communication des informations. Un tel tableau de bord permet dès lors de structurer la démarche opérationnelle en identifiant les éléments jugés nécessaires à l'anticipation du risque cyber au sein de la structure, mais également de réaliser un premier état des lieux et suivre l'avancement de chaque service dans la démarche.

2.2 Des pistes documentaires à adapter

L'anticipation du risque cyber oblige les établissements publics de santé à se doter d'un corpus documentaire permettant, à l'occasion de la survenue d'une cyberattaque, de limiter les conséquences négatives qui y seraient attachées. Il convient alors de préciser que cette démarche rédactionnelle doit nécessairement reposer sur la logique du *build and run*, c'est-à-dire construire puis enrichir et adapter.

2.2.1 Une gouvernance devant s'adapter à la spécificité cyber

A) Le rôle documentaire de la gouvernance

La gouvernance d'un établissement public de santé, particulièrement dans les suites de plans Vigipirate et d'une pandémie de COVID-19, est acculturée à la gestion de crise et a d'ores et déjà été contrainte de formaliser un certain nombre de marches à suivre dans ces situations exceptionnelles.

Laurane Raimondo rappelle toutefois que le rôle de la gouvernance en matière cyber se heurte à la limite des connaissances techniques. Aussi, la gouvernance ne peut avoir pour rôle de se substituer à la technicité du sujet. En revanche cette dernière devra s'attacher à fournir les axes et orientations à même de guider l'action technique (Raimondo, 2020). Il est également recommandé par le Guide d'élaboration du volet numérique du plan blanc de prévoir l'intégration d'acteurs techniquement experts à la cellule de crise hospitalière (CCH).

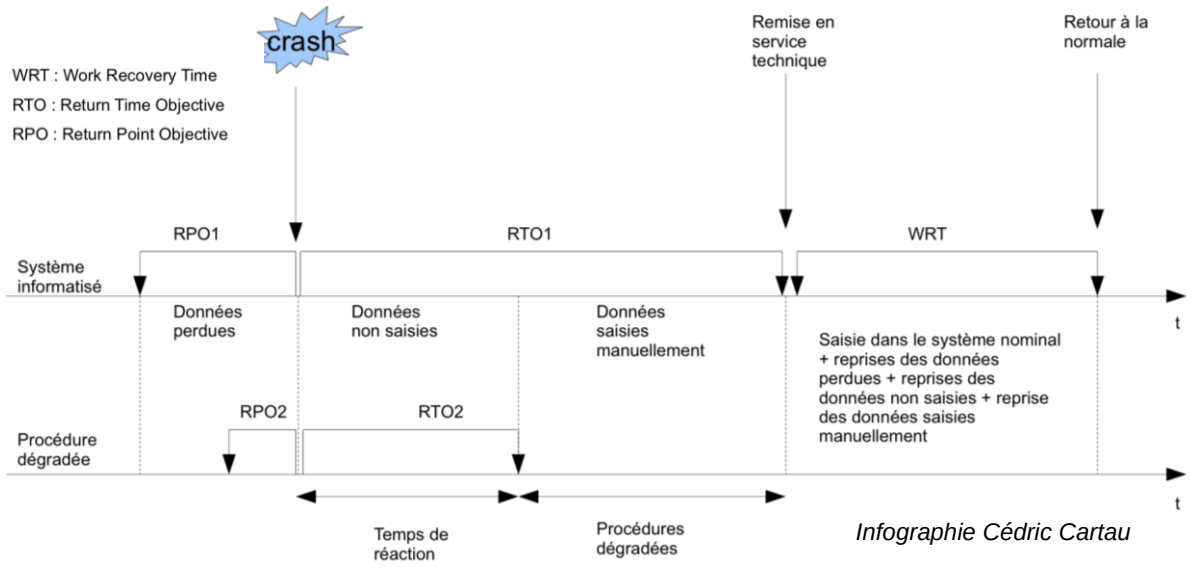
En vertu de l'article L.3110-7 du Code de la santé publique, « chaque établissement de santé est doté d'un dispositif de crise dénommé plan blanc d'établissement, qui lui permet de mobiliser immédiatement les moyens de toute nature dont il dispose en cas d'afflux de patients ou de victimes ou pour faire face à une situation sanitaire exceptionnelle ». Ce dernier doit d'ailleurs être évalué et révisé chaque année (article R.3131-13 du Code de la santé publique). La note d'information DGOS/PF/2023/94 du 15 juin 2023 témoigne alors de l'incitation ministérielle faite aux établissements de santé de se doter d'un volet numérique dans leur plan blanc.

B) Plan de continuité d'activité et plan de reprise d'activité

L'édition d'un plan blanc permet ainsi d'identifier les risques, et les éléments nécessaires à la continuité de l'activité de l'établissement lorsque l'un de ces derniers survient. La nécessité de se doter d'un plan de continuité d'activité au sein des établissements publics de santé a notamment été prégnante lors des précédentes pandémies grippales. Ce plan de continuité d'activité, défini par la norme ISO 22301 comme « la capacité de l'organisme à poursuivre la production de produits ou la prestation de services à des niveaux prédéfinis acceptables après un incident perturbateur », trouve alors toute sa place en cas de survenue d'une cyberattaque. Compte-tenu de l'envergure variable des structures, la gouvernance de l'établissement devra ainsi préalablement identifier les services producteurs nécessitant une telle planification et incluant de potentielles déprogrammations ou limites d'activité. Le rédacteur devra ensuite être identifié et, sur ce point, Cécile Weber précise que « confier cette mission à un collaborateur interne favorise un certain pragmatisme et permet d'engager une démarche de proximité avec l'ensemble des acteurs de l'organisme » (Weber, 2020 :19).

Le risque cyber met également en lumière la nécessité d'envisager le temps de la reprise de l'activité. En raison de la technicité du sujet cyber, cette coordination temporelle entre continuité et reprise apparaît primordiale en établissement public de santé. Les plans de reprise d'activité (PRA) peuvent alors se définir comme des « dispositifs opérationnels, intégrés au PCA, ayant pour objectif de faciliter le passage d'un mode dégradé à un mode de fonctionnement se rapprochant le plus possible du fonctionnement normal d'avant la crise ». Cécile Weber ajoute d'ailleurs que « d'un point de vue opérationnel, il faut accepter que la reprise d'activité ne puisse plus se faire dans les mêmes conditions, tellement les bouleversements de la crise auront été profonds » (Weber, 2020 :144).

Remise en service après crash informatique



Infographie Cédric Cartau

Cette infographie permet d'éclairer les différents temps de la crise cyber. Nous devons alors accorder toute notre attention à ce temps de *Work Recovery Time (WRT)* durant lequel, malgré un rétablissement du fonctionnement des systèmes d'information, l'ensemble des informations non saisies numériquement durant l'indisponibilité du système devront être réintégrées. Cet élément doit ainsi être incorporé à la réflexion de la gouvernance des établissements publics de santé car il est notamment susceptible d'exiger un renforcement des moyens de saisie informatique à anticiper.

C) La communication

Il est aujourd'hui communément admis que la communication constitue un réel enjeu en période de gestion de crise. Or, la réalisation du risque cyber implique de nombreuses spécificités à anticiper : coupure potentielle des moyens de communication internes comme externes, caractères techniques non maîtrisés par la gouvernance, incertitudes complexes, *etc*.

Concernant la communication vers l'extérieur, la préparation d'une trame de communiqué de presse apparaît nécessaire. Pour autant, la communication envisagée ne pourra se limiter au déclenchement de l'évènement, des informations seront attendues jusqu'au retour du fonctionnement normal de l'établissement. Plus encore, Laurane Raimondo met en exergue, au travers de l'exemple de la cyberattaque de la commune de Rolle en Suisse, les potentielles retombées médiatiques ultérieures portant sur la fuite de données (Raimondo, 2022).

La communication interne ne doit pas non plus être négligée et la gouvernance devra garder à l'esprit la nécessaire vulgarisation des éléments techniques ainsi que les canaux modifiés de diffusion d'information. Des flux pédestres de communication devront ainsi être envisagés dans un premier temps, pouvant induire des moyens humains supplémentaires.

2.2.2 Une Technique à l'épreuve rédactionnelle

Les nombreux guides édités témoignent d'un mission rédactionnelle certaine du volet technique en cas de cyberattaque. Il convient ici de s'intéresser aux principales pistes de réflexion à mener.

A) La documentation des actions internes à la DSI

L'ANSSI ainsi que les différentes certifications existantes insistent depuis plusieurs années sur la nécessité pour les DSI de connaître leurs systèmes d'information. Cette connaissance passe ainsi par l'outil de la cartographie visant à constituer un inventaire, selon différentes vues (écosystème, Métiers, applications, administration, infrastructures logiques et physiques). Soumise aux nombreuses évolutions technologiques, cette

cartographie devra nécessairement être régulièrement mise à jour. Elle revêt alors un intérêt particulier en matière d'anticipation de crise d'origine cyber en permettant une analyse de risques *a priori* sur sa vision globale du système et l'identification des briques essentielles à l'activité. A ce titre, la DSI sera amenée, en lien avec la gouvernance de l'établissement, à identifier ses SIE et prioriser les actions de restauration sur ces derniers. L'ANSSI recommande la méthode *Ebios Risk Manager* divisée en plusieurs ateliers permettant d'identifier les valeurs métiers, les sources de risques ainsi que les scénarios stratégiques et opérationnels attachés au risque afin d'anticiper leur traitement par des mesures de sécurité adaptées (ANSSI, 2018).

Une fiche réflexe synthétique est également recommandée afin d'identifier au mieux la nature d'un dysfonctionnement informatique signalé et objectiver la détection d'une cyberattaque. Dans ce cadre, il convient de souligner la récurrence des cyberattaques nocturnes, impliquant une équipe technique réduite d'astreinte. Cette piste de réflexion doit aussi inclure les acteurs à prévenir en cas de cyberattaque avérée. Une attention particulière devra être apportée à une stratégie rapide de sécurisation des sauvegardes.

La Technique devra enfin se doter d'un PRA informatique afin d'anticiper la restauration des logiciels mais également réfléchir aux modalités de récupération optimale des données qui auraient pu être endommagées ou perdues du fait de la cyberattaque.

B) La documentation des actions externes à la DSI

A l'occasion d'une crise d'origine cyber, la DSI sera fortement mobilisée par les acteurs internes impactés mais également externes à l'établissement.

Ainsi, il conviendra d'anticiper toutes les modalités de recueil de preuves de la cyberattaque pour les autorités judiciaires mais aussi les acteurs qui accompagneront la structure dans la gestion et résolution de l'incident (ANSSI, CERT-Santé notamment). Il s'agit ici d'une réflexion nécessaire à mener « à froid » pour éviter toute action hâtive durant la crise pouvant compromettre les éléments de preuve et nécessaires à la bonne restauration.

Différentes actions à destination des acteurs et services internes à l'établissement seront également à mener. Si une attention particulière doit être portée aux moyens de communication des membres de la cellule de crise hospitalière (CCH) et cellule de crise technique si existante, il convient également d'envisager les dispositifs permettant de maintenir l'activité dans le cadre d'un PCA informatique. Nous pouvons penser à la mise à disposition d'équipements informatiques non connectés au réseau afin d'accéder aux éléments qui ne seraient pas hébergés par l'établissement, la création de messageries de

substitution pour permettre le maintien d'un moyen de communication numérique, la distribution de sauvegardes imprimées des dossiers patients, *etc*. Il est important de pouvoir identifier ces actions en amont ainsi que leur priorisation et temporalité. Une communication préalable auprès des services sur le sujet est également nécessaire.

2.2.3 Une opérationnalité assurée par l'intelligibilité des documents utilisés par les Métiers

A) Typologie de rédaction et acteurs impliqués

Si les pistes de réflexions et recommandations nationales sont abondantes sur le volet technique d'anticipation du risque cyber, ce constat ne peut être similaire pour la partie opérationnelle de la documentation. En effet, le récent Guide d'élaboration du volet numérique du plan blanc, comme les entretiens menés mettent principalement en lumière l'outil opérationnel des « procédures du mode dégradé ». Il convient également de rappeler que l'édition d'une telle documentation était présentée comme indicateur du prérequis « fiabilité, disponibilité » dans le cadre du programme Hôpital numérique (HOP'EN). La fiche pratique de la boîte à outils fournie par la DGOS en 2012 afférente à l'élaboration des procédures de fonctionnement en « mode dégradé » précisait alors que « chaque service ou entité qui utilise des applications logicielles Métier critiques doit pouvoir continuer à travailler en l'absence de ces applications » (DGOS, 2012 :1). Aussi, nous pouvons présumer de l'existence contemporaine de ces procédures pour les services opérationnels identifiés comme critiques. Les incertitudes étudiées entourant la survenue d'une cyberattaque impliquent toutefois l'actuelle nécessité d'une réflexion élargie à l'ensemble des services opérationnels.

En suivant la recommandation précédemment énoncée de Cécile Weber sur l'attribution de la mission de rédaction du PCA à un collaborateur interne, nous pouvons d'ores et déjà envisager l'association pleine et entière des Métiers de l'établissement public de santé dans l'élaboration de la documentation opérationnelle. Pour autant, ces acteurs auront généralement besoin de l'appui technique de la DSI, mais également de la Direction Qualité connue pour ses compétences en matière de rédaction de procédures.

Les enjeux contemporains de développement du numérique en santé obligent toutefois les acteurs internes à l'établissement public de santé à questionner les fournisseurs d'équipement et de solutions logicielles. En effet, nous pouvons envisager de nombreux questionnements sur la continuité de l'activité d'un équipement d'imagerie par résonance magnétique (IRM) ou d'un autoclave sans possibilité de report logiciel des données. Il en va de même concernant l'indisponibilité des logiciels de traitement de paie. Le questionnement des fournisseurs sur la potentielle continuité d'activité de leurs services en

cas d'indisponibilité des systèmes d'information hospitaliers ayant pour origine une cyberattaque doit ainsi être réalisé. Plus encore, la formalisation de procédures du « mode numérique dégradé » avec ces prestataires doit pouvoir être envisagée.

B) Méthodologie de rédaction et questionnements de la disponibilité des procédures en cas d'indisponibilité des systèmes d'information ayant pour origine une cyberattaque

La rédaction devra être adaptée aux spécificités du service concerné. Il apparaît alors intéressant de partir du processus de fonctionnement nominal et identifier les points pouvant être impactés par une indisponibilité des SIH ayant pour origine une cyberattaque. L'approche *worst case* (la situation la plus défavorable) est régulièrement utilisée en matière d'anticipation de gestion de crise et doit nous amener à envisager une coupure complète de l'outil numérique et moyens de communication afférents. Des questions simples permettront aux acteurs de se projeter. Il conviendra ensuite de solutionner chacune des étapes du processus générant des difficultés dans la continuité de l'activité, en soulignant que la réduction de l'activité du service ou le transfert nécessaire des patients constituent des actions inhérentes à la construction de solutions.

La fiche pratique éditée par la DGOS permet ainsi d'éclairer les grandes notions devant être abordées :

- Les activités relatives aux échanges avec les services extérieurs ;
- Les activités propres au fonctionnement interne du service ;
- L'identification des supports techniques nécessaires au maintien de l'activité, comprenant par exemple les dossiers patients en version papier, les plans de soins, les prescriptions en cours, *etc*. ;
- Les modalités de bascule du fonctionnement en « mode dégradé » ;
- Les modalités de retour au fonctionnement nominal (DGOS, 2012).

Les réflexions menées à l'occasion de mon stage professionnel ainsi que l'entretien mené auprès de RSSI ont toutefois mis en exergue la difficulté de mise à disposition des procédures rédigées en cas d'indisponibilité des SIH ayant pour origine une cyberattaque. En effet, dans la continuité de la démarche de *build and run*, une telle documentation doit être actualisée rendant complexe son impression papier recommandée actuellement par les autorités. L'idée d'un stockage externalisé de la gestion documentaire (GED) a ainsi été soulevée afin de permettre son accès par le biais de matériels informatiques hors réseau. L'impression des supports techniques papiers préparés devra également être envisagée par le vecteur d'imprimantes déconnectées du réseau interne.

Mais la démarche de *build and run* n'implique pas seulement l'actualisation. Cette dernière doit en effet permettre d'améliorer les réponses envisagées. Le test d'une telle documentation par le vecteur de sensibilisations et d'exercices s'avère ainsi indispensable.

2.3 Sensibiliser et exercer aux fins d'améliorer

Les notions de sensibilisation et d'exercices par la simulation se sont largement développées en matière d'anticipation d'une gestion de crise. Aussi, les établissements publics de santé sont, depuis 2021, soumis à une obligation d'exercer leur(s) cellule(s) de crise (2.3.1). Pour autant, le volet technique doit également faire l'objet d'exercices particuliers, aussi dénommés tests, afin de s'assurer des réponses informatiques pouvant être apportées (2.3.2). En raison de la spécificité du risque cyber, les services opérationnels doivent être acculturés à ce sujet et développer certains réflexes (2.3.3). Il est important de souligner que ces typologies d'exercice peuvent être réalisées indépendamment les unes des autres. La finalité de ces campagnes de sensibilisation et d'exercice demeure la perspective des améliorations pouvant être apportées aux outils d'anticipation de la démarche (2.3.4).

2.3.1 L'obligation annuelle d'exercer la cellule de crise

L'instruction n° SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et à leur financement affichait une cible de 100% d'exercice de continuité d'activité en « mode numérique dégradé » à l'horizon de mai 2023 pour les OSE. Cette note d'information à destination des directions générales d'ARS précisait alors les moyens mis à disposition, à savoir un soutien financier dédié et des kits produits par l'ANS, différenciés selon le niveau de maturité de l'établissement bénéficiaire. Il convient alors de noter que le niveau confirmé vise un exercice à l'échelle du GHT.

A) <u>La portée de l'exercice annuel de continuité d'activité en « mode numérique dégradé » et son élaboration</u>

A la lecture des kits proposés par l'ANS, il convient de relever une vision principalement portée sur la coordination des cellules de crise décisionnelle, c'est-à-dire la gouvernance en situation de gestion de crise cyber. Le CHU de Reims avait toutefois fait le choix d'y adjoindre une cellule de crise technique constituée et un service opérationnel unité de soins critiques afin d'observer un certain enchaînement des réactions et actions engagées. Des stimuli préétablis sont proposés dans le kit afin de simuler une attaque de type rançongiciel. Une demi-journée est à prévoir pour la réalisation de l'exercice proposé. L'intérêt de l'utilisation de ce kit réside principalement dans la mise à disposition d'outils pratiques.

Le guide édité par l'ANSSI pour organiser un exercice de gestion de crise cyber propose toutefois différents types d'attaque et les impacts potentiels afférents pouvant rendre intéressante l'observation des réactions suscitées (ANSSI, 2020).

Une note de cadrage (annexe 7) s'avère indispensable à la bonne élaboration d'un exercice. Elle permettra d'identifier en amont :

- La date et le lieu de l'exercice ;
- Les participants et rôles de chacun (joueurs, animateurs, observateurs) ;
- Les objectifs de l'exercice ;
- La communication sur l'exercice.

La rédaction d'un scénario (annexe 8) permettra de décrire la mise en situation des joueurs, idéalement de l'évènement conduisant à l'activation de la cellule de crise à la phase de remédiation. Les premiers exercices pouvant impliquer des temps de réflexion allongés, il est préconisé de débuter par des actions simples et limitées au premier temps de la crise. Adjoindre des questions de guidage pourra aider les animateurs à faire avancer les joueurs en cas de questionnements multiples. La construction d'un tel scénario repose finalement sur l'application et le suivi des procédures éditées afin de les tester en conditions réelles.

Le recours à un chronogramme (annexe 9) permet de décrire, au moyen d'un tableur et ligne par ligne, le déroulement chronologique de l'exercice. Il permettra notamment d'identifier les moments d'envoi de stimuli. Dans son guide, l'ANSSI insiste d'ailleurs sur l'importance des stimuli de pression médiatique (ANSSI, 2020).

Un point de vigilance sera à apporter à la réunion des outils nécessaires au suivi des procédures du « mode numérique dégradé » par les joueurs. Nous pouvons par exemple penser à l'équipement de la salle de crise ou aux dossiers patients au format papier dans l'unité de soins. La question peut également se poser de la prévenance auprès des joueurs et de la mise à disposition documentaire en amont de l'exercice. Il s'agit ici d'une décision stratégique dans l'observation des biais cognitifs, les réactions pouvant être différentes lorsque l'exercice survient à l'insu des joueurs. Dans ce cas, les animateurs devront toutefois être vigilants à adopter un jeu de rôle approprié et empêcher toute communication extérieure à la simulation ne mentionnant pas le caractère d'exercice.

Il apparaît également intéressant de construire en amont une fiche d'évaluation permettant un positionnement chiffré des actions (annexe 10). Pour y répondre, le renseignement chronologique des observations devra être consigné.

B) Le choix de réaliser l'exercice avec des moyens internes ou de recourir à un prestataire extérieur

En vertu de l'instruction du 30 janvier 2023 précitée, la délégation de crédits des ARS pour la réalisation d'exercices cyber s'effectue selon deux modalités :

- Auprès du groupement régional d'appui au développement de la e-santé (GRADeS) organisant l'exercice dans l'établissement de santé ;
- Directement auprès de l'établissement de santé s'appuyant sur un prestataire extérieur pour la réalisation de l'exercice.

Pour exemple, l'appel à projets portant sur le financement d'exercices de continuité d'activité en « mode numérique dégradé » au profit des établissements sanitaire du Grand Est dont j'ai pu prendre connaissance demandait ainsi aux établissements publics de santé répondants de renseigner une grille d'autoévaluation de maturité en matière de cybersécurité et passer une commande d'accompagnement à la réalisation de l'exercice auprès de la Centrale d'achat de l'informatique hospitalière (CAIH) ou autre centrale d'achat.

Cet objectif de réalisation annuelle d'un exercice de crise d'origine cyber étant en réalité assigné depuis l'instruction n° SG/SHFDS/2021/253 du 14 décembre 2021 et faisant l'objet d'une déclaration à l'OPSSIES, les établissements publics de santé ne sont actuellement pas astreints à recourir à un prestataire extérieur.

Il ressort des entretiens menés un manque de moyens humains prégnants aux fins de réalisation de ces exercices en interne pouvant amener les établissements à reporter leur choix sur le recours à un prestataire. Pour autant, une certaine insatisfaction des RSSI a pu m'être soulignée en raison d'un manque d'adéquation de l'exercice avec le domaine sanitaire et un reste à charge financier important pour l'établissement. Les RSSI ayant réalisé cet exercice avec des moyens internes à leur établissement ont mis en avant la possibilité de diversifier les approches en proposant successivement des exercices sur table, le test précis de l'appel à l'assistance informatique suivant l'envoi d'un stimuli, la mise en pratique de l'action de récupération des plans de soins synchronisés sur un *cloud* privé, la simulation à l'échelle de l'ensemble de la structure à l'occasion d'une maintenance nécessitant une coupure réseau, un exercice dédié à la procédure de déclaration d'incident auprès des autorités, *etc*.

2.3.2 Une spécificité de la Technique à préserver dans la construction du programme d'exercices

Si la Technique doit être intégrée aux exercices de cellule de crise, sa spécificité en matière de gestion de crise cyber implique des tests distincts et particulièrement le développement de tests d'intrusion. La portée de ces tests est double : permettre d'exercer le repérage d'une cyberattaque et enrichir la documentation de management du risque numérique.

Les tests d'intrusion, désormais obligatoires dans le cadre de certifications ISO, sont généralement réalisés par un prestataire extérieur qui, après collecte des renseignements sur le SIH et analyse des failles du réseau tentera de franchir les mesures de sécurité. Il pourra ainsi être force de recommandations portant sur les risques à identifier et les mesures de sécurité à adopter ou enrichir, tant sur les volets organisationnels que procéduraux et techniques.

Pour autant, Laurane Raimondo propose de renforcer la pro-activité des équipes des DSI en leur proposant de réaliser eux-mêmes la recherche de failles et enrichir leurs connaissances du SIH. Pour cela, elle propose la formation de deux équipes techniques :

- L'équipe rouge en charge de l'identification puis de l'exploitation des failles ;
- L'équipe bleue en charge de surveiller l'activité sur le SIH et protéger les données (Raimondo, 2022).

Cette approche permet de mettre en lumière l'intérêt de tests par la simulation et notamment offrir la possibilité à l'équipe qui sera chargée de la gestion technique d'une cyberattaque de se placer en position de cybercriminel. Répondant aux mêmes objectifs que les tests d'intrusion, la plus-value d'une telle méthodologie est d'ancrer l'appropriation des mesures par une réalisation personnelle des agents.

Nous pouvons également convenir que l'exercice procédural ne nécessite aucunement l'implication systématique de la cellule de crise. Il peut par exemple apparaître pertinent de tester régulièrement les équipes de la DSI sur la pratique du report du système vers l'infrastructure de secours.

2.3.3 Des Métiers à sensibiliser et exercer dans leur opérationnalité

A) La sensibilisation des Métiers

Dans son axe 4 portant sur le déploiement d'un cadre propice pour le développement des usages et de l'innovation numérique, la Feuille de route du numérique en santé 2023-2027 souligne l'importance de la formation et la sensibilisation de tous les acteurs du sanitaire et du social à la cybersécurité et à l'hygiène informatique. Cette dernière semble se matérialiser par un objectif de réalisation d'un exercice de crise cyber annuel ou bi-annuel par l'ensemble des établissements d'ici 2027. Pour autant, il convient de ne pas délaisser les actions de sensibilisation qui, contrairement aux exercices, peuvent être généralisées en unité de temps et de lieu à l'ensemble d'un établissement.

Ainsi, les établissements publics de santé peuvent user du rappel de règles d'hygiène numérique auprès de leurs agents. Ce rappel peut s'effectuer par l'affichage des règles (annexe 11) ou encore des présentations en instances.

Plus encore, des prestataires proposent aujourd'hui le déploiement de campagnes de sensibilisation par l'action en permettant l'envoi d'e-mails reproduisant les techniques de *phishing*. L'agent cliquant sur le lien contenu sera alors redirigé vers une page de sensibilisation. Dans ce développement de *nudges* (annexe 1) permettant aux bénéficiaires d'actionner eux-mêmes leur formation, nous pouvons également retrouver la mise à disposition de visuels accessibles types « bouton rouge » directement dans les e-mails afin de signaler toute suspicion de tentative de *phishing*. Rendre cette fonctionnalité immédiatement actionnable peut encourager le signalement par les utilisateurs.

La sensibilisation des Métiers portera donc principalement sur les comportements à adopter en tant qu'utilisateurs du SIH afin de limiter les risques d'intrusion.

B) L'exercice des Métiers au « mode numérique dégradé »

Les exercices, en revanche, visent à tester les procédures établies en cas de survenue d'une cyberattaque. Leur conception est alors similaire à celle envisagée précédemment pour la ou les cellule(s) de crise (note de cadrage, chronogramme, grille d'observation, *etc*.). Comme évoqué précédemment, il peut être intéressant d'établir un programme d'exercice par service opérationnel mais également un ordre de priorité temporel. Aussi, la première campagne d'exercices pourrait principalement porter sur les services utilisateurs des SIE identifiés, ou du moins un échantillon représentatif de ces derniers si nous considérons, par exemple, le nombre important de services faisant usage du dossier patient informatisé.

Le CHU de Reims avait ainsi pu cibler des services pilotes :

- Des services administratifs de traitement de paie ;
- Des services médico-techniques : un secteur d'imagerie médicale, un bloc opératoire, un secteur du laboratoire de biologie médicale, l'unité de stérilisation et la pharmacie à usage intérieur ;
- Des services de soins critiques et d'urgence : réanimation, SAMU ;
- Des services de soins conventionnels : un service de consultation, un service d'hospitalisation.

Compte-tenu de la diversité des domaines d'activité abordés, un entretien préalable avec l'encadrement et le responsable de structure interne du service concerné s'avère nécessaire (annexe 12). Il permet de connaître l'avancement des acteurs dans la démarche, notamment en matière de rédaction de procédures du « mode numérique dégradé ». Il est toutefois possible que ces derniers souhaitent bénéficier d'un premier exercice aux fins d'enclencher la rédaction des procédures en tirant les enseignements d'une mise en situation. Cette approche doit permettre au coordonnateur de la démarche opérationnelle de se positionner en qualité d'accompagnant.

Pour autant, il convient de préciser que, si la simulation en santé est principalement reconnue pour transférer « des apprentissages du milieu de formation vers le milieu de soins » (Jaffrelot, Pelaccia, 2016 :18), l'approche de la simulation d'une crise s'avère différente. Comme le soulignent Elsa Gisquet et Olivier Borraz, « il s'agit de tester et d'entraîner les participants à développer des capacités d'agilité dans une situation marquée par l'incertitude […]. Il ne s'agit pas de dire ce qui pourrait être, de manière à envisager des solutions de prévention, mais de projeter les participants dans une situation perturbée et instable, de manière à les entraîner à y faire face » (Gisquet, Borraz, 2020 :387). En effet, les scénarios des exercices en services opérationnels doivent s'efforcer de laisser une certaine latitude à l'expression des biais cognitifs induits par la gestion de crise et à la création de réflexes intuitifs au travers de la simulation. Il conviendra d'enrichir les procédures du « mode numérique dégradé » par ces observations.

2.3.4 Penser l'après : de la déstabilisation aux améliorations

En matière d'exercice ou de tests, tout comme à l'issue d'une réelle crise d'origine cyber, la réflexion dédiée à l'amélioration à l'occasion du retour d'expérience (RETEX) s'avère être la composante essentielle de la résilience attendue des établissements publics de santé. Cette phase doit en effet permettre de partager les constats collectifs et individuels des participants et engager les acteurs à solutionner les difficultés rencontrées.

Comme le souligne Anaïs Gautier, « l'interaction confère du sens à l'organisation en raison du partage qu'elle permet par l'expression de chacun des membres de ses perceptions et de ses interprétations de la situation. […] la vision commune de la situation doit permettre l'action collective en toute rationalité donc le maintien de la structure organisationnelle quel que soit l'environnement, calme ou turbulent » (Gautier, 2012 :196). Le RETEX doit ainsi permettre le partage d'une vision personnelle des participants à l'exercice mais également la construction collective de réactions appropriées en situation de gestion de crise.

Le guide de l'ANSSI dédié à l'organisation d'un exercice de gestion de crise cyber fait par ailleurs mention de la nécessaire organisation d'un tel RETEX composé d'un temps de *débriefing* « à chaud » dans les suites immédiates de la fin de l'exercice puis d'un RETEX « à froid » dans les jours ou le mois suivant(s) permettant la production d'un support de restitution. Lorsque l'exercice implique plusieurs cellules de crise ou services opérationnels, l'organisation d'un RETEX commun constituera une réelle plus-value permettant à différents profils d'une même organisation de se rassembler autour de la question cyber (ANSSI, 2020). Les échanges se tenant à l'occasion d'un RETEX doivent être structurés et tracés par une personne identifiée préalablement.

Le *débriefing* « à chaud » consiste généralement en un tour de table permettant à chaque participant de s'exprimer. Les éléments soulevés seront ensuite réinvestis pour le RETEX « à froid » devant engager les propositions d'améliorations par les participants. La production concomitante d'un support de restitution abordant les objectifs atteints, non atteints et les actions d'amélioration envisagées témoigne alors de l'importance de capitaliser sur l'expérience vécue et il convient de réfléchir à ses modalités de partage. Pour exemple, le groupe de travail pluridisciplinaire créé durant mon stage et composé de différents profils opérationnels était bénéficiaire des RETEX d'exercices réalisés dans les services et présentés par une partie des joueurs. Cette restitution permettait un enrichissement mutuel des participants au groupe par le partage commun de points de vigilance et pistes d'amélioration. La restitution devra également être dirigée vers les acteurs identifiés dans l'appui à la démarche, qu'elle soit stratégique, technique ou opérationnelle.

L’édition d’un plan d’actions priorisées et temporellement délimitées ainsi que la désignation d’un ou plusieurs acteurs internes chargés du suivi son exécution consacrent enfin l’aboutissement de la démarche d’amélioration continue induite par l’anticipation d’une crise d’origine cyber.

Les outils d’anticipation d’une crise d’origine cyber sont ainsi multiples et surtout à adapter aux ressources et spécificités locales de l’établissement public de santé. Au regard des enjeux que revêt le risque cyber ainsi que la multitude d’acteurs devant être impliqués dans l’anticipation de ses conséquences, il revient au Directeur d’hôpital d’investir cette thématique par le vecteur du renforcement de la fiabilité et de la résilience de son organisation.

3 Mise en perspective des enjeux locaux, territoriaux et nationaux : capitaliser sur l'anticipation du risque cyber pour gagner en fiabilité et résilience

L'approche complexe de la gestion de crise soulevée par Laurane Raimondo et son analogie aux HRO mises en regard avec une pandémie mondiale ou la menace grandissante de cyberattaques doivent permettre au Directeur d'hôpital d'envisager une nouvelle vision des organisations hospitalières dans une optique de résilience accrue. Aussi, l'anticipation du risque cyber tend aujourd'hui à apparaître comme un marqueur de fiabilité d'un établissement public de santé (3.1). Cette démarche devra toutefois intégrer à terme une vision territoriale élargie, seule à même de garantir un niveau de résilience acceptable (3.2).

3.1 L'anticipation du risque cyber comme vecteur de fiabilité d'un établissement public de santé

3.1.1 Un rapprochement du risque cyber aux situations sanitaires exceptionnelles, gage d'une fiabilité locale dans l'anticipation de la gestion de crise

A) Une incitation au rapprochement rédactionnel

L'incitation nationale à l'élaboration d'un volet numérique du plan blanc apparaît comme un révélateur de l'appariement de la gestion de crise cyber à la gestion des SSE. Initiée par la loi n°2004-806 du 9 août 2004 relative à la politique de santé publique, la planification de la réponse aux SSE s'est considérablement étoffée au fil du temps et des épisodes de déstabilisations de l'organisation hospitalière. En 2014 a ainsi été instauré le dispositif régional d'organisation de la réponse sanitaire (ORSAN) afin d'améliorer la réponse régionale à cinq typologies de situations sanitaires exceptionnelles (SSE) impliquant des prises en charge spécifiques et/ou massives.

Si le risque cyber ne peut, de prime abord et par son essence, s'apparenter à cette composante du plan blanc, la logique d'anticipation de la réponse apportée est similaire. L'application à l'anticipation de la gestion de crise cyber d'une méthodologie éprouvée en matière de SSE permet ainsi son intégration au plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles.

La logique des analyses de risques portée sur la cartographie des SIH par le Guide d'aide à la préparation du plan blanc numérique rejoint également celle appliquée aux SSE par l'évaluation d'un niveau de probabilité de risques. Complété par l'identification des impacts résultant de la réalisation du risque et son niveau de gravité selon la méthode *Ebios Risk Manager* publiée par l'ANSSI, le cadrage rédactionnel de l'anticipation d'une crise d'origine cyber s'inscrit dans les recommandations faites en matière de SSE.

B) Un rapprochement organisationnel à envisager

Le Guide d'aide à la préparation et à la gestion des tensions hospitalière et des situations sanitaires exceptionnelles édité en 2019 par la Direction générale de la santé (DGS) et la Direction générale de l'offre de soins (DGOS) fait état de la constitution d'une équipe projet pour l'élaboration du plan, son actualisation et l'organisation d'exercices. Cette équipe est composée d'un chef de projet, idéalement Directeur, dont la désignation doit être portée à la connaissance de l'ARS, mais également de référents SSE. Selon ces recommandations, les référents SSE sont des « professionnels de santé (médecin, pharmaciens, cadres de santé, infirmiers, ingénieurs en gestion de risque…) ou tout autre personnel d'encadrement qualifié dans les domaines des SSE » (DGS, DGOS, 2019 :33). Peuvent également s'adjoindre à l'équipe « toute personne ressource en fonction des volets spécifiques » (DGS, DGOS, 2019 :33) et le Directeur médical de crise.

Parallèlement, le guide d'aide à la préparation du plan blanc numérique édité par la DGOS en 2023 fait état du rôle du RSSI devant entre autres « mettre en place des mesures visant à limiter la survenue d'un incident numérique et de cyberattaque en particulier » et mener « régulièrement des actions de sensibilisations et d'information, des simulations » (DGOS, 2023 :6). Ce dernier était par ailleurs d'ores et déjà mentionné dans le guide destiné aux SSE afin de participer à l'équipe constituée en qualité de personne ressource pour « assurer l'interopérabilité des dispositifs de prise en charge des victimes » (DGS, DGOS, 2019 :33).

Nous pouvons ainsi convenir d'un rôle complémentaire de l'équipe SSE et du RSSI dans l'anticipation du risque cyber et la planification des réponses apportées, qu'il s'agisse de l'anticipation de modalités organisationnelles comme le transfert massif de patients vers un autre établissement ou de la mise en œuvre d'exercices. Cette complémentarité doit cependant être élaborée et facilitée compte-tenu des différents liens hiérarchiques dont relèvent l'équipe SSE et le RSSI. Cette démarche n'est alors aucunement aisée dans un questionnement latent de valorisation de cette activité d'anticipation et de gestion de crise.

C) L'entrée du « risque numérique » dans la certification de la Haute Autorité de Santé

La récente mention du risque numérique (critère 3.6-02) dans la version 2023 du Manuel de Certification des établissements de santé pour la qualité des soins édité par la HAS au côté du critère impératif de gestion des tensions hospitalières et des SSE (critère 3.6-01) témoigne de cette accointance mais également du vecteur de fiabilité que représente l'anticipation du risque cyber. Les éléments d'évaluation du critère 3.6-02 « Les risques numériques sont maîtrisés » reposent alors sur la déclaration des incidents à l'ANS et la mise en œuvre des recommandations de l'ANSSI mais également la maîtrise des conduites à tenir et la connaissance des mesures de prévention du risque par les équipes. Nous constatons ainsi une avancée opérationnelle dans les critères d'évaluation. En effet, si certaines versions antérieures de la certification HAS avait pu aborder le volet informatique sous l'angle documentaire (rédaction d'un PRA, analyse de risques numériques par exemple), la mise à jour 2023 impulse une nouvelle dynamique de connaissance et de maîtrise des procédures du « mode numérique dégradé ».

Aussi, qu'il s'agisse de l'anticipation des réponse apportées à une SSE ou à la réalisation d'un risque cyber, la certification HAS des établissements de santé constitue un indice non négligeable sur son niveau de fiabilité en matière de qualité et de sécurité des soins. Plus encore, les résultats de ces certifications sont aujourd'hui accessibles au grand public via le site d'information Qualiscope. Les usagers du système, incités par les politiques publiques à devenir acteurs de leurs parcours, sont ainsi davantage sensibilisés à la qualité des soins offertes par les établissements de santé. Dès lors, l'anticipation du risque cyber et plus largement des conséquences susceptibles de déstabiliser le fonctionnement d'une structure dans une optique de résilience sont désormais une composante de cette qualité des soins recherchée.

3.1.2 Un appui régional et national croissant mais encore jugé insuffisant dans cette quête à la fiabilité cyber

Force est alors de constater l'investissement croissant des autorités publiques nationales dans cette démarche de gain en fiabilité cyber des établissements publics de santé. Comme étudié précédemment, le déploiement du numérique en santé est présenté comme un gage de qualité de notre système de santé permettant aux usagers d'être acteurs de leur santé, aux professionnels de renforcer leur cohésion et aux institutions de faciliter la circulation de l'information. L'incitation à l'usage de technologies créées par le niveau national est ainsi à observer et permettent de garantir un niveau vérifié de cybersécurité. En témoigne ainsi la mise en service de quatre solutions nationales de partage représentant près de 2 milliards d'euros d'investissement : le dossier médical partagé (DMP) aujourd'hui intégré à Mon

espace santé, la messagerie sécurisée de santé « MSSanté », l'Identité Nationale de Santé (INS) et le dispositif Pro Santé Connect (PSC).

Plus encore, nous pouvons souligner deux nouveaux financements forfaitaires issus du Ségur du numérique afin d'encourager l'usage de ces solutions nationales :

- Un financement à l'équipement permettant d'acquérir les dernières versions logicielles référencées par l'ANS en matière de DPI, de référentiels d'identités, de système de gestion de laboratoire et de système d'information de radiologie.
- Un financement à l'usage du DMP et de MSSanté. Ce dernier tend d'ailleurs à intégrer le dispositif des incitations financières à la qualité et à la sécurité des soins (IFAQ) pour l'année 2023.

Reste pour autant en suspens la question de la sécurisation d'autres solutions logicielles voire matérielles connectées ne résultant pas de financements étatiques dédiés et dont les établissements publics de santé demeurent consommateurs. A ce titre, nous pouvons souligner une réflexion nationale d'édition de référentiels opposables, notamment le salué référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques approuvé par un arrêté du 22 février 2023.

Pour autant, les moyens réglementaires et financiers étatiques ne sauraient suffire aux établissements publics de santé dont les ressources et compétences humaines permettant de les mettre en application s'avèrent largement insuffisantes. Les agences nationales que sont l'ANSSI et l'ANS ou régionales créées avec la figure du groupement régional d'appui au développement de la e-santé (GRADeS) n'ont en effet qu'un rôle d'accompagnement jugé limité par les RSSI interrogés. Ce raisonnement se vérifie d'ailleurs dans la difficile valorisation de l'activité d'anticipation de la gestion de crise cyber au sein des établissements de santé. Ainsi, les établissements publics de santé sont-ils actuellement confrontés à des injonctions contradictoires. D'une part, la sécurisation nécessaire à toute administration pour laquelle ces derniers ne disposent pas des outils étatiques dédiés. Nous pouvons penser aux solutions ministérielles internes déployées pour les transferts sécurisés de documents par exemple. D'autre part, la spécificité du domaine sanitaire obligeant à une approche particulière de l'anticipation du risque cyber à laquelle peu de prestataires extérieurs peuvent répondre.

Il convient ainsi, en conservant les vecteurs de fiabilité locaux, régionaux et nationaux, de gagner en résilience par l'investissement d'une dynamique territoriale d'anticipation du risque cyber et une implication citoyenne grandissante.

3.2 L’enjeu de la cybersécurité à investir territorialement pour gagner en résilience

Si la résilience dont doivent faire preuve les établissements publics de santé en matière de gestion de crise d’origine cyber induit une fiabilité entreprise en amont de la crise par la sécurisation et l’anticipation, cette dernière devra également s’exprimer en intégrant les acteurs territoriaux du système de santé, tant professionnels (3.2.1) qu’usagers (3.2.2).

3.2.1 Une nécessaire réflexion territoriale des professionnels de santé

Les outils d’anticipation présentés précédemment reposent sur des observations et une consultation menée auprès de RSSI mettant en lumière une dynamique actuelle essentiellement intra-établissement (locale). Aucun exemple de maturité permettant une structuration aboutie de la démarche opérationnelle au niveau du GHT n’a pu être apporté. Il s’agit pourtant d’un objectif induit par la convergence des SIH et les kits d’exercice produits par l’ANS. Le gain en résilience ne pourra alors s’affirmer sans une harmonisation des pratiques d’anticipation à l’échelle du GHT. Cette notion rejoint ainsi la nécessité de disposer de compétences et ressources humaines dans l’ensemble des établissements parties. Plus encore, la diffusion de RETEX doit être organisée à cette échelle élargie afin de favoriser une dynamique de réflexion commune. Il convient d’ajouter que la spécificité du risque cyber induit la possibilité d’une crise élargie au GHT ayant des SIH unifiés (DGOS, 2016) qui doit donc être anticipée à cette échelle.

Aussi, les autres acteurs présents sur le territoire seront susceptibles d’être mobilisés. Nous pouvons aisément penser aux établissements de santé privés et aux établissements d’hébergement pour personnes âgées dépendantes (EHPAD) offrant des prises en charge médicalisées. Les inclure à cette réflexion apparaît aujourd’hui nécessaire en cas de transferts de patients à anticiper par exemple. Cette anticipation territoriale doit d’ailleurs être réciproque car toute structure sanitaire, sociale ou médico-sociale subit la menace du risque cyber.

Les professionnels de santé libéraux sont également des acteurs du territoire qu’il convient de mobiliser dans l’anticipation du risque cyber. Tout d’abord par une communication privilégiée en cas de survenue d’une cyberattaque paralysant les SIH pour adresser les patients mais également une sensibilisation à la sécurisation de l’usage des outils numériques de liaison ayant vocation à s’étendre dans les prochaines années. Le risque cyber doit permettre de capitaliser sur ces échanges en matière de gestion de crise afin d’offrir un territoire armé et organisé aux usagers du système de santé.

3.2.2 Une sensibilisation au risque cyber devant être élargie à la population

L'article L.1111-1-1 du Code de la santé publique débute en précisant qu'un « service public, placé sous la responsabilité du ministre chargé de la santé, a pour mission la diffusion gratuite et la plus large des informations relatives à la santé et aux produits de santé ». Il s'agit également d'un des objectifs poursuivis par le déploiement du numérique en santé visant à garantir une meilleure diffusion de l'information en santé. Compte-tenu des dernières cybermenaces usant du déploiement de ce nouveau vecteur d'information pour attaquer les individus eux-mêmes, les autorités publiques nationales ont investi le terrain de la prévention des risques numériques liés au système de santé. En témoignent les campagnes nationales relayées dans les établissements de santé à l'instar des visuels Tous cybervigilants (annexe 13). Mais la feuille de route précitée insiste désormais sur l'initiation de cette sensibilisation devant être portée par les établissements public de santé auprès de tous les citoyens usagers du numérique en santé. Elle fixe pour objectif un taux de 80% d'établissements sanitaires et médico-sociaux ayant mis en place des actions de sensibilisation d'ici fin 2027. Ainsi, au-delà du lieu de soins, l'établissement public de santé est considéré comme le relai national de la promotion du numérique en santé, mais il apparaît alors nécessaire d'y adjoindre une composante de prévention du risque cyber lié à son usage.

Un tel raisonnement permet d'alimenter un cercle vertueux visant à déployer à une échelle nationale la sensibilisation au risque cyber. Nous avons en effet constaté que les intrusions ne dépendaient pas uniquement de l'établissement public santé ou de l'institution touchée. L'ensemble des remparts structurels mis en place ne sauraient suffire à limiter le risque de cyberattaque. Aussi, l'éducation de la population aux règles d'hygiène numérique est nécessaire. Ce constat se vérifie d'ailleurs lorsque nous envisageons que tout citoyen est amené à occuper un emploi au sein des institutions ciblées par les cyberattaques. Cette éducation peut ainsi également trouver à s'appliquer dans l'enseignement primaire et secondaire pour former les futurs professionnels. Nous détenons ainsi une première brique d'alimentation du cercle vertueux. En poursuivant cette réflexion, nous pourrions également convenir que l'éducation au risque cyber est susceptible de faire naître de nouveaux métiers. En prenant le prisme privilégié du système de santé, les établissements ont aujourd'hui tout intérêt à multiplier les partenariats avec les écoles d'ingénierie numérique aux fins de proposer des axes spécifiques à la cybersécurité en santé. Les RSSI interrogés ont ainsi pu mettre en avant les récentes politiques de développement des contrats d'apprentissage au sein des DSI. Ces recrutements non pérennes ouvrent toutefois la voie à une nouvelle technicité admise au sein des établissements publics de santé.

Enfin, une sensibilisation au risque cyber en établissement public de santé élargie à la population permettrait d'investir davantage la communication en situation de gestion de crise auprès des usagers du système de santé. Chaque citoyen, en vertu du onzième alinéa du Préambule de la Constitution de 1946, dispose du droit à la protection de sa santé. Or, nous avons vu que cette dernière pouvait être menacée par le risque cyber. Nous devons ainsi rappeler que la conséquence négative à éviter prioritairement en matière de gestion de crise d'origine cyber est la perte de chance pour le patient. Nous sommes alors collectivement encouragés à envisager la compréhension d'un tel scénario par la population au travers d'outils de communication et de messages adaptés mais également, et surtout, d'une concertation et sensibilisation préalables.

Conclusion

La menace de la cyberattaque pesant sur les établissements publics de santé est ainsi multiforme, de même que les conséquences pouvant être engendrées par cette dernière. Les enjeux induits par la survenue de ce risque imposent aux établissements publics de santé de se préparer, dans cette spécificité de l'incertitude et d'un sujet aux multiples combinaisons possibles. Le choix du *worst case* est récurrent en matière de gestion de crise afin de permettre de se préparer à la situation la plus défavorable, mais il ne doit pas occulter l'idée que toute crise apportera son lot de conséquences négatives comme positives.

Les HRO nous démontrent que les turbulences auxquelles elles peuvent être confrontées les font finalement progresser. C'est ainsi vers cette approche complexe de la crise que les établissements publics de santé doivent se diriger en matière cyber. En effet, si la cyberattaque ne peut être évitée avec certitude, la crise qu'elle génère est évitable par l'anticipation des conséquences afférentes, prioritairement négatives. L'objectif de tout établissement public de santé réside aujourd'hui dans la possibilité de se doter d'outils à même d'envisager les actions à mener en cas de dysfonctionnement de ses SIH mais également de réduire les biais cognitifs induits par un tel évènement. Dans sa résilience, l'établissement public de santé confronté à une cyberattaque devra ainsi accepter l'incident, mettre en œuvre ses actions anticipées et tirer profit des améliorations nécessaires.

Plus encore, nous pouvons convenir que l'anticipation du risque cyber constitue un élément sur lequel tout établissement public de santé peut capitaliser. Il en ressort un renforcement de la cohésion locale en investissant les réflexions techniques, Métiers et de gouvernance mais également territoriale en construisant collectivement une réponse organisationnelle.

Enfin, la Directive européenne NIS 2 a vocation à élever l'ensemble des établissements de santé au rang régalien d'« entité essentielle », alors que seuls les établissements supports de GHT étaient aujourd'hui considérés comme « opérateurs de services essentiels ». Tournée vers un approfondissement de l'approche qualité et gestion des risques dans une optique de renforcement de la résilience, cette perspective prochaine d'application au mois d'octobre 2024 doit conforter le directeur d'hôpital dans la nécessité d'investir localement et territorialement l'anticipation de la gestion de crise d'origine cyber.

Bibliographie

Références juridiques

Directive UE 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Network and Information Security – NIS 1).

Directive UE 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, modifiant le règlement UE910/2014 et la directive UE 2018/1972 et aborgeant la directive UE 2016/1148 (Network and Information Security – NIS 2).

Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

Code de la santé publique

Code pénal

Code de la défense

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

Loi n°2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

Ordonnance n°2021-1574 du 24 novembre 2021 portant partie législative du code général de la fonction publique.

Décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature.

Arrêté du 13 décembre 2016 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle des ministères chargés des affaires sociales

Arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé ».

Arrêté du 22 février 2023 portant approbation du référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques.

Arrêté du 17 avril 2023 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Etablissements de santé ».

Instruction n° SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information («plan d'action SSI») dans les établissements et services concernés.

Instruction n°SG/DSSIS/2017/8 du 10 janvier 2017 relative à l'organisation à déployer pour la mise en œuvre de la stratégie d'e-santé en région.

Instruction n°DGS/VSS2/DGOS/2019/167 du 26 juillet 2019 relative à l'actualisation du cadre de préparation du système de santé à la gestion des tensions hospitalières et des situations sanitaires exceptionnelles.

Instruction n°SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et à leur financement

Note d'information n° DGOS/PF/2023/94 du 15 juin 2023 visant à informer les établissements de santé de la publication d'un guide d'aide à la préparation au volet numérique du Plan blanc.

Accord relatif à la mise en œuvre du télétravail dans la fonction publique, 3 avril 2022.

Ouvrages

ARPAGIAN N., 2022, La cybersécurité, Collection Que sais-je ?, Presses universitaires de France

RAIMONDO L. (dir), 2022, Les fondamentaux de la gestion de crise cyber, Ellipses.

VINCK D. 2016, Humanités Numériques : La culture face aux nouvelles technologies, Le Cavalier Bleu.

WEBER C., 2020, Plan de continuité des activités et gestion de crise, Afnor Editions.

Articles de périodiques, revues

ALEXANDER R., DONADILLE L., 2022, "Cyberattaque : retour d'expérience du centre hospitalier d'Arles", Risques et qualité en milieu de soins vol. 19 n°1, p33-37.

BEVIERE-BOYER B., 2021, « La gestion des données de santé par le Health Data Hub : le recours à la société Microsoft, entre risques et précautions », Droit, Santé et Société n°3, p.42-48.

CAUSSE J.D., 2013, « Krisis : jugement et promesse », Revue d'éthique et de théologie morale n°276, p.295-302.

CASSOU-MOUNAT B., 2019, "La sécurité numérique en établissement de santé : comment s'y préparer ?", Techniques hospitalières n°778, p.21-26.

CHAUVIN S., IGONETTI J.B., 2020, « Comment associer la DSI et les Métiers pour exploiter au mieux les données que génère toute activité humaine ? », La Revue des Sciences de Gestion (n°301-302), p.77-84.

DE BOVIS C., 2009, « D'une prévention des risques classiques à des organisations à haute fiabilité », Management et Avenir n°27, p. 241 à 259.

DOUZET F., 2014, « La géopolitique pour comprendre le cyberespace », Hérodote n°152-153, p.3-21.

DOUZET F., 2020, « Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique », Hérodote n°177-178, p3-15.

FEVRIER R., 2020, « Covid-19 et cyberattaques : Vers une nécessaire évolution du paradigme dominant en management stratégique ? », Revue française de gestion n°293, p.81-94.

FRANCOIS S., 2022, “Cyberattaque au Centre hospitalier universitaire de Rouen : Retour d’expérience”, Risques et qualité en milieu de soins vol. 19 n°1, p23-25.

GAUTIER A, 2012, « Théorisation d’une pratique de retour d’expérience organisationnel : Comment éclairer le sens de l’action dans les comportements en situation ?», Revue internationale de psychosociologie et gestion des comportements organisationnels, vol. 18, p.193-221.

GISQUET E., BORRAZ O., 2020, « Simuler une crise : la construction de la réalité dans les exercices d’accident nucléaire », Sociologie vol. 11, p.385-398.

GODART J., 2022, “D’une cyber-catastrophe à l’opportunité d’un nouveau modèle évolutif au centre hospitalier de Wallonie picarde”, Risques et qualité en milieu de soins vol. 19 n°1, p29-32.

HOUTAIN S., 2022, “Cybersécurité : ne vaut-il pas mieux prévenir que guérir ?”, Risques et qualité en milieu de soins vol. 19 n°1, p12-16.

HOUTAIN S., 2022, “Cyberattaque d’un établissement : quelle conduite en pratique ?”, Risques et qualité en milieu de soins vol. 19 n°1, p17-22.

JAFFRELOT M., PELACCIA T., 2016, « La simulation en santé : principes, outils, impacts et implications pour la formation des enseignants », Recherche et formation n°82, p.17-30.

LEGROS P., 2022, « L’impératif de sécurité des données de santé, de la nécessité technique à l’obligation juridique », Revue internationale de droit économique, p.13-37.

LEMESLE A., TERRIEN N., LUCAS M., BROWAEYS L., 2022, “Par le jeu, rien n’est impossible ! L’escape game “Sant’escape - Sécurité numérique” déployé en région Pays de la Loire”, Risques et qualité en milieu de soins vol. 19 n°1, p38-44.

MARTINEZ F., 2010, « L'individu face au risque : l'apport de Kahneman et Tversky », Idées économiques et sociales n°161, p.15-23.

MESZAROS T., DE COLIGNY A., 2015, « Perceptions, décisions et rationalité dans la gestion des crises », Stratégique n°110, p.139-151.

MOISDON J.C, 2020, « Régulation et gestion de la qualité des soins dans les établissements de santé. Une comparaison avec le secteur nucléaire », Journal de gestion et d'économie de la santé n°4, p.275-287.

MORIN E., 2012, « Pour une crisologie », Communications n°91, p.135-152.

Etudes, rapports, guides, feuilles de route

ANSSI, 2018, « Cartographie du système d'information. Guide d'élaboration en 5 étapes ».

ANSSI, 2018, « La méthode EBIOS Risk Manager – Le Guide ».

ANSSI, 2019, « La méthode EBIOS Risk Manager – Fiches méthodes ».

ANSSI, 2019, « Maîtrise du risque numérique - l'atout confiance ».

ANSSI, 2020 « Organiser un exercice de gestion de crise cyber ».

ANSSI 2021, « Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique ».

ANSSI, 2023, Panorama de la cybermenace 2022.

ATIH, 2021, Atlas des SIH 2020.

CARTAU C., 2021, Guide cyber résilience opus 2, 2ème édition.

DGOS, 2016, « GHT Mode d'emploi. Guide méthodologique : stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT ».

DGOS, 2012, « Boîte à outils pour l'atteinte des pré-requis – Fiches pratiques, Programme Hôpital numérique ».

DGOS, 2023, « Plan blanc numérique – Etablissements de santé - Guide d'aide à la préparation ».

DGOS, 2023, « IFAQ 2023 : Guide de présentation et de remplissage des indicateurs numériques ». Disponible à l'adresse : https://www.fhf.fr/sites/default/files/2023-06/IFAQ%202023_Guide%20indicateurs%20numeriques%202023%20VF.pdf

DGS, DGOS, 2019, « Guide d'aide à la préparation et à la gestion des tensions hospitalières et des situations sanitaires exceptionnelles ».

DGS, 2019, « Guide méthodologique - Retour d'expérience situations d'urgence sanitaire et exercices de simulation ».

Direction interministérielle de la transformation publique, 2021, « Objectif 0 papier : une guide pour simplifier et dématérialiser vos processus internes ».

Ministère de la santé, 2019, « Feuille de route Accélérer le virage numérique 2019-2022 ».

Ministère de la santé, 2023, « Feuille de route du numérique en santé 2023-2027 ».

Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social, 2023, Rapport public 2022. Disponible à l'adresse : https://esante.gouv.fr/espace-presse/lobservatoire-des-incidents-de-securite-des-systemes-dinformation-pour-les-secteurs-sante-et-medico-social-2022-est-en-ligne

PON D., COURY A., 2019 « Accélérer le virage numérique ».

Conférences, colloques, webinar, déclarations

CALMES G., CHAUDRON E., DUHESME L., LE GLOAN C., MILLET C., 2023, Cycle de conférences sur la sécurité : "Le défi de la cybersécurité à l'hôpital", AEDH EHESP.

FABRE J., 2023, Conférence cybersécurité « Professionnels de santé, évitons le chaos ! », Union hospitalière de Cornouaille avec l'appui du GCS e-Santé Bretagne et l'APSSIS. Disponible en rediffusion à l'adresse : Conférence Cybersécurité Quimper le 28/06/2023

TERRADE N., 2023, Cyberattaque au CH de DAX : Retour d'expérience et enseignements 2 ans après, Groupe PSIH. Disponible en rediffusion à l'adresse : https://app.livestorm.co/groupe-psih/cyberattaque-au-ch-de-dax-retour-dexperience-and-enseignements-2-ans-apres/live

Déclaration de M. Emmanuel Macron, président de la République, sur la mobilisation face à l'épidémie de COVID-19, Paris, le 16 mars 2020. Disponible à l'adresse : https://www.vie-publique.fr/discours/273933-emmanuel-macron-16-mars-2020-coronavirus-confinement-municipales

Déclaration de M. Emmanuel Macron, président de la République, sur les cyberattaques dans les hôpitaux et la stratégie nationale pour la cybersécurité, à Paris le 18 février 2021. Disponible à l'adresse : https://www.vie-publique.fr/discours/278659-emmanuel-macron-18022021-cybersecurite

Sites internet

www.sante.gouv.fr
www.esante.gouv.fr
www.ssi.gouv.fr
www.health-data-hub.fr
www.has-santé.fr

Liste des annexes

Annexe 1 : Glossaire

Advanced persistent threats ou menace persistante avancée : typologie de virus informatique visant un certain niveau de technicité et de pérennité du piratage afin d'agir sans autorisation sur un système d'information et/ou d'en extraire des données.

Bruteforce attack ou technique de la force brute : pratique de piratage informatique visant à tester chaque combinaison possible d'un mot de passe ou d'une clé pour identifiant donné afin de se connecter au service ciblé.

Cheval de Troie : typologie de virus informatique introduit dans un programme informatique légitime.

Keylogger ou enregistreur de frappe : logiciel espion capable de détecter et enregistrer les saisies de l'utilisateur d'un système d'information sur son clavier.

Nudges ou coup de pouce : outils visant à modifier les comportements quotidiens d'un individu sous la forme d'une incitation discrète. Ils sont considérés comme facilitateurs de la prise de décisions peu intuitives ou difficiles à prendre.

Phishing ou hameçonnage : cyberattaque consistant à obtenir d'un individu ses identifiants d'accès à des comptes personnels et/ou professionnels en utilisant une couverture jugée légitime.

Ransomware ou rançongiciels : typologie de virus informatique, le *ransomware* vise à perturber le fonctionnement normal d'un système informatique en conditionnant sa reprise nominale au paiement d'une rançon.

Rootkit ou outil de dissimulation d'activité : typologie de virus informatique permettant de pérenniser un accès non autorisé et invisible à un système d'information.

Virus informatique : programme informatique malveillant introduit à l'insu du propriétaire du système.

Annexe 2 : Synthèse des réunions du groupe de travail pluridisciplinaire « exercices cyber » du CHU de Reims

Date de la réunion	Présentations	Arbitrages
22/02/2023	*Contexte *Etat des lieux de l'existant *Objectifs sur groupe	*Cibler les services non impactés par le déménagement. *Identifications de typologies services pilotes. *Intégration d'un représentant des usagers.
22/03/2023	*Distinction SIE et logiciels critiques. *Services pilotes volontaires. *Proposition d'un kit unifié (grille d'entretien préalable, note de cadrage, évaluation, fiche d'observation, fiche RETEX).	*Validation du principe de kit unifié, à présenter à la prochaine réunion. *Validation des services pilotes désignés.
04/05/2023	*Présentation du kit unifié. *Retour du cadrage de deux exercices pilotes programmés. *Information du cadrage du test des cellules de crise + unité de soins. *Retour entretien service administratif : besoin en procédures avant exercice.	*Validation du kit unifié présenté. *Groupe de travail bénéficiaire des RETEX. Privilégie les RETEX par les participants à l'exercice. *Nécessité de recenser les procédure mode numérique dégradé disponibles dans les services.
06/07/2023	*Actualisation des SIE. *RETEX exercice stérilisation. *RETEX tests cellules de crise + unité de soins. *Bilan premier semestre 2023 et perspectives.	*Contenu du tableau de bord de suivi opérationnel. *Priorisation des exercices du second semestre.

Annexe 3 :Questionnaire électronique

Enquête mémoire EDH - Démarche anticipation crise cyber

Bonjour,

Dans le cadre de la rédaction de mon mémoire de fin de formation d'élève-directeur d'hôpital "*Cyberattaque en établissement public de santé : anticiper les conséquences de l'inéluctable*", je souhaite soumettre à différents acteurs de ce domaine le présent questionnaire portant sur la démarche, stratégique comme opérationnelle, mise en place dans votre établissement.

Je vous remercie par avance pour le temps que vous pourrez y accorder,

Diane VERES

Début — Terminé

Nom de votre établissement et GHT :

Qui coordonne, en propre, au sein de votre établissement, la démarche stratégique afin d'anticiper la crise cyber ? *

- ☐ Chef d'établissement en propre
- ☐ Direction des systèmes d'information/services numériques
- ☐ Direction Qualité Gestion des Risques
- ☐ RSSI
- ☐ COPIL dédié
- ☐ Autre (à préciser)

(Suivi des actions, organisation des réunions, ...)

Réponse si autre :

Quelle démarche stratégique permet de cadrer l'anticipation de la crise cyber dans votre établissement ? *

- ○ Gestion des SSE
- ○ Démarche ad hoc (à préciser)

Réponse si "démarche ad hoc"

Quel corpus documentaire stratégique et opérationnel avez-vous mis en place pour anticiper la crise cyber ? *

- ☐ Projet d'établissement
- ☐ Projets des services opérationnels (y compris administratifs)
- ☐ Projet médico-soignant partagé du GHT
- ☐ Cartographie des risques
- ☐ PCA
- ☐ PRA
- ☐ GED procédures mode dégradé cyberattaque (métiers et techniques)
- ☐ Autres (à préciser)

Réponse si autre

Quelles démarche de sensibilisation au risque cyber avez-vous déployé au sein de votre établissement ? *

Quelles sont les modalités de réalisation des exercices ? *

- ☐ Les exercices sont organisés avec nos ressources internes
- ☐ Les exercices sont réalisés par un prestataire extérieur
- ☐ Nous n'avons pas encore réalisé d'exercice

Merci d'expliciter le choix de la modalité de réalisation des exercices (pourquoi ? comment ?)

Si les exercices sont réalisés avec vos ressources internes, pourriez-vous me décrire la démarche utilisée ?

(Fréquence, effectifs animateurs/observateurs, services pilotes, tableau de bord de déploiement des exercices, ...)

En cas de non-conformité(s) identifiée(s), qui est chargé de l'élaboration et du suivi du plan d'actions correctives ? *

- ☐ Agent(s) Direction Qualité Gestion des Risques
- ☐ Agent(s) Direction de systèmes d'information/services numériques
- ☐ Equipe SSE
- ☐ RSSI
- ☐ Personne pour le moment
- ☐ Autre personne

Réponse si autre personne

Comment envisagez-vous le déploiement des outils d'anticipation de la crise cyber au niveau de votre GHT ? *

Selon vous, quelle progression pourrait être apportée à la démarche nationale en matière d'outils d'anticipation et de gestion de crise cyber ? *

Si vous le souhaitez, merci de bien vouloir me communiquer votre courriel

Objectifs : temps d'échange portant sur les réponses apportées, communication ultérieure du mémoire, ...

Soumettre

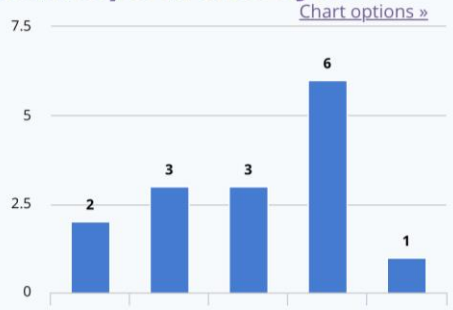
Annexe 4 : Résultats du questionnaire électronique

Nombre de répondants : 6

<u>Réponses aux questions fermées :</u>

Qui coordonne, en propre, au sein de votre établissement, la démarche stratégique afin d'anticiper la crise cyber ?

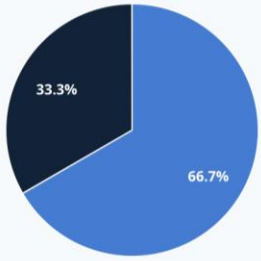
Chart options »



Chef d'établissement en propre	2
Direction des systèmes d'information/services numériques	3
Direction Qualité Gestion des Risques	3
RSSI	6
COPIL dédié	1

Quelle démarche stratégique permet de cadrer l'anticipation de la crise cyber dans votre établissement ?

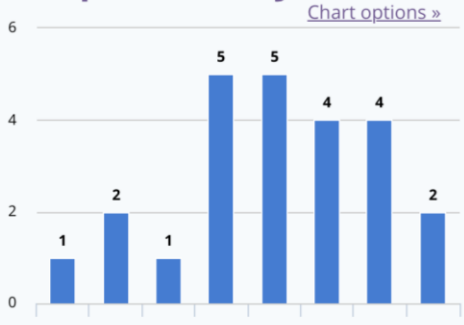
Chart options »



Gestion des SSE	4
Démarche ad hoc (à préciser)	2

Quel corpus documentaire stratégique et opérationnel avez-vous mis en place pour anticiper la crise cyber ?

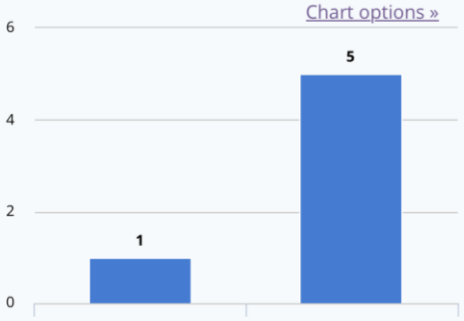
Chart options »



Projet d'établissement	1
Projets des services opérationnels (y compris administratifs)	2
Projet médico-soignant partagé du GHT	1
Cartographie des risques	5
PCA	5
PRA	4
GED procédures mode dégradé cyberattaque (métiers et techniques)	4
Autres (à préciser)	2

Quelles sont les modalités de réalisation des exercices ?

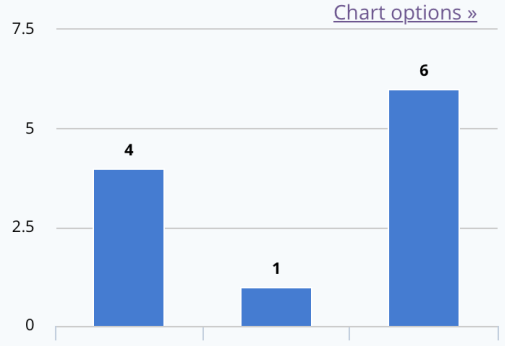
Chart options »



Les exercices sont organisés avec nos ressources internes	1
Les exercices sont réalisés par un prestataire extérieur	5

En cas de non-conformité(s) identifiée(s), qui est chargé de l'élaboration et du suivi du plan d'actions correctives ?

Chart options »



Agent(s) Direction de systèmes d'information/services numériques	4
Equipe SSE	1
RSSI	6

Réponses aux questions ouvertes :

	Qui coordonne, en propre, au sein de votre établissement, la démarche stratégique afin d'anticiper la crise cyber ?	Quelle démarche stratégique permet de cadrer l'anticipation de la crise cyber dans votre établissement ?	Quel corpus documentaire stratégique et opérationnel avez-vous mis en place pour anticiper la crise cyber ?	Quelles démarche de sensibilisation au risque cyber avez-vous déployé au sein de votre établissement ?	Merci d'expliciter le choix de la modalité de réalisation des exercices (pourquoi ? comment ?)
	Réponse si autre :	Réponse si "démarche ad hoc"	Réponse si autre :		
1	Coordination de sécurité bi-mensuelle par établissement	la cyberattaque est un scénario du plan blanc	sauvegarde des premières mesures vers un cloud souverain / heure	sensibilisation direction / mails / notes	RSSI certifié, exercice sur table avec les directions et admin de garde
2			Plan de Crise Cyber associé à une Gestion Opérationnelle de Crise	fishing, cours pour les étudiants, interventions lors de réunions institutionelles	
3				Affichages, Flyers, Escapes Games, Exercices de *Phishing*, exercice de crise, sensibilisation présentielles	Obligation suivie par l'ARS
4			Démarche en cours, le corpus documentaire n'a pas été formalisé	présentation de la démarche en directoire, bureau de CME	exercice kit ANS débutant au regard de notre maturité
5		Analyse de risque EBIOS RM		MOOC	Temps nécessaire pour la préparation que le RSSI n'a pas.
6			Plan "Hôpital sans informatique"	Sensibilisation SSI en ligne pour tous les utilisateurs, Cours SSI au IFPS, campagne de mails	Cadre réglementaire : Exercice rédigé par l'ANS et financé par l'ARS. 1 fois par an

	Si les exercices sont réalisés avec vos ressources internes, pourriez-vous me décrire la démarche utilisée ?	En cas de non-conformité(s) identifiée(s), qui est chargé de l'élaboration et du suivi du plan d'actions correctives ?	Comment envisagez-vous le déploiement des outils d'anticipation de la crise cyber au niveau de votre GHT ?	Selon vous, quelle progression pourrait être apportée à la démarche nationale en matière d'outils d'anticipation et de gestion de crise cyber ?
		Réponse si autre personne :		
1	scénario avec plusieurs input, outils (teams, fiches pratiques) par rôle, facilitateurs, observateurs, minutiers...	Plan d'action, et d'amélioration après retex à chaud et à froid	Sensibilisation + formation / cloud / smartphone / pc déconnecté	Ressources humaines, financières + réduction du RTO pour le PCA mutualisation du PRA
2			Il faut mettre en accord les 7 Entités Juridiques... compliqué...	une initiative nationale, un guide ou une plateforme sécurisée souveraine à exploiter
3			Fiches du PSSE validées en instance, fiches PCA construite et validée par les services.	Imposer aux directions non récéptrice une réelle prise en charge des plan de sécurisation
4	exercice kit ANS débutant au regard de notre maturité		je ne comprends pas la question	je ne comprends pas la question
5			Avec un manque de RH interne pour les opérer.	Faire que cela soit introduit dans la démarche SSE
6			Via la coordination COMOP SSI GHT	Il y a eu beaucoup d'amélioration déjà faite dans la structuration et la la coordination nationale et régionale de l'appui SSI

Annexe 5 : Grille d'entretien semi-directif

Temps estimé : 2 heures

Vous êtes un groupe régional de RSSI. Au carrefour des démarches stratégique, technique et opérationnelle, votre point de vue ainsi que vos interactions m'intéressent. La restitution de notre entretien sera anonymisée. Nous resterons vigilants à respecter un tour de table à chaque questionnement. Sentez-vous libre de rebondir sur les propos échangés.

Renseignements sur la vision et la pratique du métier de RSSI

1) Pourriez-vous me présenter votre mission de RSSI et votre GHT ?
2) Depuis combien de temps exercez-vous ce métier ? Que faisiez-vous avant ?
3) Avez-vous des outils de partage de pratiques et d'expériences entre vos GHT ?

Questionner la démarche locale voire GHT d'anticipation du risque cyber

4) Comment se sont matérialisées vos démarches stratégique, technique et opérationnelle en matière d'anticipation du risque cyber ?
5) Êtes-vous associés à la démarche stratégique en qualité de RSSI ? Comment ?
6) Une ou plusieurs de ces trois démarches sont-elle structurées à l'échelle de votre GHT ?

Questionner la documentation existante en matière d'anticipation de la gestion de crise cyber

7) De quel corpus documentaire disposez-vous en matière d'anticipation de la gestion de crise cyber ?
8) Avez-vous une vision sur les procédures « mode numérique dégradé » Métiers ?

Questionner la méthodologie de réalisation des exercices de gestion de crise cyber

9) Avez-vous fait appel à un prestataire extérieur ou usé de ressources internes pour la réalisation des exercices ?
10) Un service opérationnel a-t-il déjà bénéficié d'un exercice ?
11) La même méthode a-t-elle été retenue pour l'ensemble du GHT ?

Recueillir l'avis des RSSI sur les moyens nationaux et régionaux investis

12) Comment percevez-vous les récents investissements et outils nationaux/régionaux en matière d'anticipation du risque cyber ?

Annexe 6 : Visuels campagne de prévention nationale relative aux risques et recommandation de l'exercice d'une activité télétravail

Source : www.cybermalveillance.gouv.fr

Annexe 7 : Note de cadrage exercice cyber obligatoire – Exemple du CHU de Reims

Exercice cyber

Note de cadrage

Cyberattaque
CCH, CCDSN et unité de soins

Définition des caractéristiques de l'exercice	
Contexte	Cyberattaque entraînant l'impossibilité d'accéder au réseau internet/intranet du CHU.
Objectif principal	S'assurer de la communication ascendante et descendante entre les acteurs. *-Détail des objectifs à atteindre et leur évaluation en annexe 1-*
Objectif secondaire	Vérifier l'applicabilité et l'adéquation des procédures mode dégradé.
Enjeux	S'assurer des modalités de continuité d'activité et de l'anticipation des conséquences en cas de cyberattaque.
Nature	Obligatoire (instruction du 30/01/2023)
Cadre et paramètre de l'exercice	
Lieu	Salle crise CCH + salle de crise DSN + unité de soins
Date	Anonymisé
Horaires	Anonymisé
Scénario	
Joueurs	Directeurs, agents DSN, agents unité de soins
Animateurs	• CCH : Anonymisé • CC DSN : Anonymisé • Unité de soins : Anonymisé
Evaluateurs	• CCH : Anonymisé • CC DSN : Anonymisé • Unité de soins : Anonymisé
Observateurs	• CCH : Anonymisé • CC DSN : Anonymisé • Unité de soins : Anonymisé
Autres participants	Observation médicale en sus
Cadence de l'exercice	*Cf annexe 2*

Actions attendues	*Cf annexe 1*
Moyens nécessaires à l'exercice	
Humains	Aucun moyen humain supplémentaire nécessaire
Matériels	Toutes les procédures mode dégradé papier.
Coûts et financement	0
Condition d'animation et d'observation de l'exercice	
Rôle de l'animateur	• CCH : guider au besoin • CC DSN : guider au besoin • Unité de soins : jeu de rôle étudiant, question en conséquence à poser pour encourager la réflexion si besoin. Aucune intervention permettant d'identifier un exercice.
Rôle de l'évaluateur	• CCH : traçabilité du niveau de réussite selon annexe fournie • CC DSN : traçabilité du niveau de réussite selon annexe fournie • Unité de soins : jeu de rôle étudiant ; traçabilité du niveau de réussite selon annexe fournie.
Rôle des observateurs	Observer, tracer de manière chronologique les actions et échanges.
Documents à fournir et/ou à préparer	Procédures mode dégradé imprimées, matériel mentionné dans les procédures mode dégradé
Réunion de calage en amont de l'exercice	• Anonymisé • Anonymisé
Modalité d'évaluation de l'exercice	
Débriefing	• A chaud par secteur. • A froid secteurs réunis dans les 2 à 3 semaines suivant exercice. • Partage RETEX unité de soins en groupe de travail entraînements cyber. • Partage RETEX COPIL SSE.
Communication	Plateforme OPSSIES.
Outils et critères d'évaluation	*Cf annexe*

Annexe 8 : Scénario exercice cyber obligatoire – Exemple du CHU de Reims

Annexe 2 :

Scénario

Unité de soins

1. **Envoi du stimuli au service**

2. **Service doit alerter directeur de garde de l'impossibilité d'accéder au réseau + message reçu**

Question guidage :
- Qui devez-vous prévenir ?
- Où trouvez-vous le numéro ?
- Quel téléphone utilisez-vous ?

3. **Service doit appliquer son fonctionnement en mode dégradé le temps de la résolution du problème**

Question guidage :
- Où trouver la procédure dégradée ?
- Comment prévenir toute l'équipe ?
- Rappel de personnel nécessaire ?
- Nécessité en déprogrammation/réduction voire arrêt accueil/transfert à 4 heures, 72 heures, 2 mois ?

CCDSN

1. **Réception et qualification de l'incident relayé par le directeur de garde**

- Comment qualifiez-vous l'incident (solliciter les avis de la procédure) ?

2. **Réflexe de l'isolement des systèmes infectés/non infectés et alerte des équipes**

- Comment isolez-vous le système infecté ? Comment préservez-vous
- Qui prévenez-vous ?
  - ☐ Equipes Datacenter et VDI ou à défaut responsable infrastructure.
  - ☐ Directeur DSN.

3. **Réflexe déclenchement cellule de crise DSN**

- Qui la déclenche ?
- Où vous rendez-vous ? Avec qui ?
- Que faites-vous dans la salle de réunion ? (cocher :)
  - ☐ Ouverture de l'armoire CC DSN
  - ☐ Installation des clés 4G
  - ☐ Installation des PC de remédiation
  - ☐ Mise en évidence des documentations et cartographies
- Comment assurez-vous la traçabilité des échanges et des actions ?

4. **Déclaration et demande d'aide**

  - ☐ Appel au CERT-SANTE
  - ☐ Déclaration d'incident à l'ANS
  - ☐ Prévenir le DPD en cas de violation de données

CCH

1. **Réception de l'appel de l'unité de soins par le directeur de garde et déclenchement de la cellule de crise**
  - ☐ Prévenir la DSN
  - ☐ Utiliser MENKORN

2. **Accéder à la salle institutionnelle du pôle de biologie et l'installer**

- Où trouvez-vous les clés ?
- Que devez-vous installer ?
- Comment pouvez-vous vous assurer que toutes les parties prenantes sont présentes ?

3. **Communiquer**

- Avec qui communiquez-vous par ordre de priorité ?
- Par quels moyens communiquez-vous ?
- Quel niveau de détails donnez-vous ?

Annexe 9 : Extraits de chronogramme – Exemple du guide ANSSI

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
1	AAMMJJ 09:30	Début de l'exercice	*« Bonjour, l'exercice commence maintenant. N'hésitez pas à nous contacter pour toute question ou incompréhension. »*	DIRANIM	Tous les joueurs	Mail	Aucune action particulière attendue.	
2	AAMMJJ 09:32	Premiers messages sur l'incident	*« Bonjour, Je vous appelle car les membres de mon équipe ne peuvent plus utiliser leur ordinateur. Tous affichent un même message demandant une rançon pour récupérer les données. On a un projet très important à rendre en fin de semaine, il faut absolument qu'on puisse travailler. Que devons-nous faire ? Par ailleurs, je crois que le problème s'étend au moins à tout notre étage… »*	Manager d'une équipe de l'organisation [service/département au choix]	Directeur de la ligne métier/activité concernée	Appel téléphonique	Signalement/échange avec le RSSI.	Stimulus à multiplier (par intervalles de 5 à 10 minutes) autant que jugé utile (en fonction du nombre d'activités concernées ou encore de la pression souhaitée sur les joueurs). L'objectif de ces stimuli est de montrer que tous les services de l'organisation sont progressivement touchés. Il est possible d'ajouter des conséquences métiers spécifiques à chaque service dans le script des appels téléphoniques et des mails.
3	AAMMJJ 09:35	Premiers messages sur l'incident	*« Bonjour, Je vous appelle car nous avons reçu depuis ce matin plusieurs appels de salariés qui ne pouvaient plus utiliser leur ordinateur. D'après les photos reçues, les données seraient chiffrées et pourraient être récupérées en cas de paiement d'une rançon. Êtes-vous au courant de cette situation ? Nous commençons à être saturés par le volume des appels et n'avons aucune information à transmettre sur la situation… »*	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission de l'alerte et déclenchement de la cellule de crise.	Il peut être intéressant de jouer la mobilisation de la cellule de crise. Cette dernière peut être activée entre ce stimulus et le stimulus 12. Passé ce dernier, le cellule d'animation devra insister pour qu'une cellule de crise se réunisse le plus rapidement possible.
4	AAMMJJ 09:40	Premiers messages sur l'incident	*« Bonjour, À la suite de notre échange téléphonique, vous trouverez ci-joint une photo de l'un des postes. N'hésitez pas à me transmettre toute consigne qui me permettra de répondre aux futurs appels des salariés. Je vous rappelle si d'autres services nous informent qu'ils sont touchés. Nous sommes vraiment saturés par le volume d'appels et n'avons aucune information sur la situation. »*	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Mail	Estimation des premiers impacts, lancement des investigations, préparation des premières mesures de gestion de l'incident et définition consignes à destination des employés. Éventuellement, prise de contact avec un prestataire ou avec l'ANSSI (simulés par la cellule d'animation).	En fonction du logiciel malveillant choisi lors de la conception du scénario, il est possible d'utiliser des captures d'écran de rançongiciel trouvées sur Internet. Pour obtenir plus d'informations sur les bonnes pratiques à mettre en place dans le cadre d'une attaque par rançongiciel, consulter le guide de l'ANSSI *Attaques par rançongiciels, tous concernés ?*
5	AAMMJJ 09:45	Premiers messages sur l'incident	*« Bonjour, Je vous informe que les postes de travail de l'ensemble de mon équipe sont inutilisables et affichent tous le même message. Impossible de travailler. Est-ce qu'on a été piraté ? Avez-vous la possibilité de résoudre ça assez rapidement car nous devons rendre notre dossier en fin de semaine ? On a essayé de redémarrer sans succès les PC. »*	Manager d'une équipe de l'organisation [service/département au choix]	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Prise en compte de l'information et transmission des premières consignes si définies.	
6	AAMMJJ 09:50	Premiers messages sur l'incident	*« Bonjour, À la suite de notre appel, je confirme que les postes de travail de l'ensemble de mon équipe sont inutilisables et affichent tous le même message. Je vous envoie par SMS une photo de l'un des postes. Que se passe-t-il ? »*	Manager d'une équipe de l'organisation [service/département au choix]	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Prise en compte de l'information et tranmission à la cellule de crise.	
7	AAMMJJ 09:55	Premiers messages sur l'incident	*« Rebonjour, Au vu des appels reçus jusqu'ici, les services/départements X et Y sont touchés ainsi que l'équipe projet Z qui doit rendre ses conclusions en fin de semaine (indiquer une échéance critique). Pouvez-vous me transmettre des consignes afin que mon équipe puisse répondre aux interrogations des utilisateurs ? Nous nous sommes saturés et plus rien ne semble fonctionner. »*	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission des premières consignes si définies, interrogations sur le périmètre de l'attaque et début des reflexions sur la continuité d'activité.	
8	AAMMJJ 10:00	Latéralisation du rançongiciel	*« Bonjour, L'ensemble des équipes du service X n'a plus accès aux données de ses ordinateurs suite à l'affichage d'un message demandant une rançon. Nous étions en train de finaliser le projet Y que nous devions absolument rendre ce jour. Comment faire pour continuer à travailler ? Que se passe-t-il ? Je vous envoie par SMS une photo d'un écran d'un des ordinateurs inutilisables. »*	Manager d'une équipe de l'organisation [service/département au choix]	Directeur de la ligne métier/activité concernée	Appel téléphonique	Transmission des informations au RSSI et diffusion des consignes si définies.	
9	AAMMJJ 10:05	Latéralisation du rançongiciel	*« Bonjour, L'ensemble des équipes du service X n'a plus accès aux données de ses ordinateurs suite à l'affichage d'un message demandant une rançon. Que se passe-t-il ? Quand pourrons-nous reprendre le travail ? »*	Manager d'une équipe de l'organisation [service/département au choix]	Directeur de la ligne métier/activité concernée	Appel téléphonique	Transmission des informations au RSSI et diffusion des consignes si définies.	

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
23	AAMMJJ **13:40**	**Sollicitations internautes réseaux sociaux**	*« Bonjour,* *Voici quelques exemples de sollicitations que l'on trouve sur les réseaux sociaux :* *@organisation vous confirmez avoir été hacké ? #cyberthreat* *@organisation vous comptez payer la rançon ? #prisedotage #transomware*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Prise en compte de l'information dans la stratégie de communication.	
24	AAMMJJ 13:50	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Latéralisation du rançongiciel**	*« Bonjour,* *L'ensemble des postes de travail du site sont HS, ils affichent tous le même écran qui nous demande de verser une rançon. Impossible de continuer à travailler, le site est à l'arrêt ! Les commandes/services ne pourront pas être prêts à temps, c'est la catastrophe. Pouvez-vous envoyer une équipe pour y remédier ? Est-ce que le siège a le même problème ? Nous n'avons pas plus d'information en l'état, nous sommes complètement dans le flou sur l'origine du problème. »*	Équipe technique second site	RSSI / DSI si pertinent second site ou équivalent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Si non réalisé précédemment, transmission de l'alerte, déclenchement de la cellule de crise du second site et partage de l'information avec l'organisation.	Comme pour le site principal de l'organisation, les planificateurs de l'exercice devront décider en amont si le second site a toujours accès à sa messagerie. Si oui, les échanges peuvent continuer comme précédemment. Sinon, la cellule de crise du second site devra mettre en place d'autres outils pour communiquer. Il convient également de matérialiser la perte d'accès au réseau : les ordinateurs, les outils de la cellule de crise, les annuaires, la messagerie etc. ne seront plus utilisables s'ils sont gérés sur le réseau. Les joueurs devront ainsi penser à des solutions de secours pour gérer la crise et maintenir certaines activités critiques.
25	AAMMJJ **14:00**	***[Option « Simulation ANSSI »]*** **Prise de contact de la COM**	*« Bonjour,* *Je travaille au sein de la division de la communication de l'ANSSI et je prends contact avec vous suite aux échanges que vous avez avec l'agence sur votre incident. On se propose de vous accompagner pour anticiper et/ou préparer vos éléments de communication externe et interne en cas de visibilité de l'attaque.* *Des premiers éléments de communication interne ou externe ont-ils déjà été transmis ? Avez-vous été sollicité par les médias ? Pour construire votre stratégie de communication, plusieurs actions à mener dans un premier temps : définition des parties prenantes (interne, clients, autorités, etc.), des cibles et objectifs de votre communication ainsi que des éventuels points de vigilance spécifiques à votre entité (notoriété/image de marque, exposition médiatique), votre secteur d'activité (actualités du marché, etc.), votre calendrier (obligation de communication financière, rachat, etc.), etc. Nous pouvons vous accompagner dans la rédaction de vos éléments de communication (communiqué de presse, communication interne). Si vous souhaitez mentionner l'ANSSI, nous demanderons à valider la mention. »*	ANSSI COM	Responsable communication	Appel téléphonique	Elaboration de la stratégie de communication et transmission des informations au second site.	La posture générale de l'ANSSI est d'accompagner l'organisation mais pas de communiquer à sa place.
26	AAMMJJ **14:20**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Èléments sur la suspension des activités du second site**	*« Bonjour,* *À la suite de l'incident en cours depuis ce matin, voici un point de situation des impacts recensés :* *Exemples :* *- impossible de prendre les commandes (ou de les suivre) ;* *- impossible de marquer des produits et donc de les émettre ;* *- activités en mode dégradé/à l'arrêt ;* *- etc. »*	Manager d'une équipe du second site [service/département au choix]	Chef cellule de crise second site ou représentant métier en cellule de crise	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Réflexion sur la continuité d'activité.	Impacts à définir en fonction des spécificités de votre organisation et de votre second site et à décliner en autant de stimuli qu'il y a d'impacts souhaités.
27	AAMMJJ **14:35**	**Sollicitation presse**	*« Bonjour,* *Nous avons appris que votre organisation venait d'être la cible d'une cyberattaque et que les attaquants ont publié un ultimatum : payer la rançon ou voir vos données publiées en ligne. Confirmez-vous ces informations ? Cette attaque a t-elle un impact conséquent sur votre organisation ? Qui en est à l'origine selon vous ?»*	Journaliste (presse spécialisée)	Responsable communication	Appel téléphonique	Transmission des éléments de langage préalablement définis ou renvoi vers un communiqué de presse si publié.	
28	AAMMJJ **15:00**	**Sollicitation presse**	*« Bonjour,* *Pour information, nous venons d'identifier la parution d'un article dans la presse relatif à l'incident en cours. L'article met particulièrement en cause nos capacités à répondre à l'incident et à y remédier. »*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication + RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Transmission des éléments de langage préalablement définis ou renvoi vers un communiqué de presse si publié.	Ces sollicitations de la presse peuvent également être adressées au second site.
29	AAMMJJ **15:15**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Sollicitation presse**	*«Bonjour,* *Nous avons appris que votre site venait d'être victime d'une cyberattaque. Confirmez-vous cette information ? Cette attaque est-elle liée à celle ayant touché le siège ce matin ? Etes-vous en mesure de poursuivre votre activité ?»*	Journaliste	Équipe communication du second site	Appel téléphonique	Utiliser (si transmis) les EDL du siège ou les demander avant de répondre. Renvoyer à un communiqué de presse commun si existant.	

Annexe 10 : Evaluation exercice cyber obligatoire – Exemple du CHU de Reims

Annexe 1 :

Détail des objectifs à atteindre et leur évaluation pour chaque acteur.

1. Cellule de crise hospitalière (CCH)

- **Réception de l'information et alerte de la DSN**

  → Disponibilité 1 2 3
  Commentaires :

  → Réflexe du contact de la DSN avec moyen communication adapté 1 2 3
  Commentaires :

- **Déclenchement de la cellule de crise**

  → Réflexe du recours à MENKORN 1 2 3
  Commentaires :

  → Temps de connexion et d'envoi de la demande 1 2 3
  Commentaires :

  → Information ARS/préfecture 1 2 3
  Commentaires :

- **Accès à la salle institutionnelle du Pôle de Biologie**

  → Trouver la clé 1 2 3
  Commentaires :

  → Rassembler l'ensemble de la CCH en salle 1 2 3
  Cocher :
  - Directeur de garde
  - Directeur médical de crise
  - Coordonnateur des soins
  - Directeur de la communication
  - Directeur DPAL
  - Directeur DAF
  - Directeur DRH
  - Directeur DSN
  - Logisticien

  Commentaires :

  → Respect de la disposition établie dans la salle 1 2 3
  Commentaires :

- **Vérification des éléments nécessaires (fiche réflexe et installation logisticien)**

  → Papier, crayons, paper-board, … 1 2 3
  Commentaires :

  → Disponibilité du téléphone et fiches d'enregistrement des appels 1 2 3
  Commentaires :

  → Restauration 1 2 3
  Commentaires :

  → Installation des équipements 1 2 3
  Cocher :
  - Rideaux fermés
  - Disposition des banettes

- **Communication**

  → Identification des rôles de chacun dans la CCH (référent communication, rédaction des CR, …) 1 2 3
  Commentaires :

  → Détention de la liste des numéros de téléphone 1 2 3
  Commentaires :

  → Interne 1 2 3
  Commentaires :

  → Externe (patients, médias) 1 2 3
  Commentaires :

  EVALUATION : /48

- **Déclaration et demande d'aide**

→ Réflexe 1 2 3
Commentaires :

- **CCDSN et CCH arrivent à communiquer** 1 2 3
Commentaires :

EVALUATION : /30

2. Cellule de crise DSN (CCDSN)

Réception, qualification de l'incident et isolement des SI

→ L'agent support comprend et analyse le message relayé par le directeur de garde 1 2 3
Commentaires :

→ Le chaîne d'expertise trace son analyse de qualification 1 2 3
Commentaires :

→ Le responsable DSN et les équipes du data center sont prévenus dans les meilleurs délais 1 2 3
Commentaires :

→ La nécessité de protéger les SI dans les meilleurs délais est mentionnée 1 2 3
Commentaires :

Déclenchement de la cellule de crise

→ La CCDSN est constituée dans un délai raisonnable 1 2 3
Commentaires :

→ Etude de la nécessité de rappel en personnels 1 2 3
Commentaires :

→ La connaissance de la composition de la CCDSN et sa liaison avec la CCH est connue 1 2 3
Commentaires :

→ Le matériel nécessaire est installé dans les meilleurs délais 1 2 3
Cocher :
- ☐ Clés 4G
- ☐ PC de remédiation
- ☐ Documentations et cartographies

Commentaires :

→ Les échanges et actions sont tracés 1 2 3
Commentaires :

Unité de soins

- **Réflexe à l'absence d'accès réseau et au stimuli**

  → Communication au directeur de garde 1 2 3
  Commentaires :

  → Communication aux équipes de l'unité 1 2 3
  Commentaires :

- **Application du fonctionnement en mode dégradé**

  → L'emplacement des procédures est connu 1 2 3
  Commentaires :

  → L'emplacement des documents papiers est connu 1 2 3
  Commentaires :

  → La nécessité en rappel de personnels est évaluée 1 2 3
  Commentaires :

  → Des transferts sont envisagés 1 2 3
  - ☐ Oui
  - ☐ Non
    - A 2 heures
    - A 72 heures
    - A 2 mois

  → Une réduction de l'accueil est envisagée 1 2 3
  - ☐ Oui
  - ☐ Non
    - A 2 heures
    - A 72 heures
    - A 2 mois

  EVALUATION : /21

Aborder le temps de la reprise estimé selon le niveau de réussite du service.

Annexe 11 : Communication interne des règles d'hygiène numérique – Exemple du CHU de Reims

CYBER-SÉCURITÉ AU CHU DE REIMS

Ne communiquez jamais votre mot de passe

Votre mot de passe est personnel, ne l'écrivez pas, ne le « prêtez » pas à vos collègues.
A savoir ! Jamais le service informatique ne vous demandera de communiquer votre mot de passe, ni au téléphone, ni par email, ni par un formulaire à remplir.

Réfléchissez toujours avant de cliquer

Les emails, pièces-jointes et liens internet peuvent contenir des virus : prenez toujours un moment de réflexion avant de cliquer !

Protégez les données des patients

Utilisez uniquement les messageries de santé cryptées (Apicrypt / MSSanté) pour envoyer des données des patients.
N'envoyez jamais les données vers des messageries autres (Gmail, Hotmail...) et vers des espaces de stockage dans le cloud.

Attention aux clés USB

Les clés USB, disques durs externes... sont des forts vecteurs de contamination. Ne les utilisez jamais sur les ordinateurs de l'établissement. Ne branchez jamais une clés USB trouvée, même chez vous ! Certaines clés sont abandonnées uniquement dans le but de prendre en otage vos données !

Pas de rechargement par prise USB

Ne connectez jamais vos téléphones ou montres connectées en USB aux ordinateurs du CHU pour les recharger : cela laisse la porte ouverte aux attaques informatiques !

Annexe 12 : Grille d'entretien de cadrage d'un exercice en service opérationnel – Exemple du CHU de Reims

Exercice cyber

Annexe note de cadrage

Questions types - Entretien avec le service participant

Composition groupe entretien :

- ☐ 1 DSN.
- ☐ 1 SSE
- ☐ 1 chef de service/secteur/unité concerné.
- ☐ 1 cadre de proximité du service/secteur/unité concerné.
- ☐ Si présents, 1 à 2 internes ou étudiants en santé du service/secteur/unité concerné.

- Définir le moment opportun pour l'entraînement et non le plus confortable.
  Paramètres à prendre en compte :
  - Activité du service.
  - Présence de personnels.

- Lieu de l'entraînement
  - ☐ Dans le service.
  - ☐ Hors du service dans salle de simulation dédiée.

- Eléments à maintenir qui seront nécessaires pour la prise en charge des urgences pouvant survenir pendant l'entraînement :
  - ..
  - ..
  - ..
  - ..
  - ..
  - ..

- Vérification du matériel nécessaire à l'application des procédures en mode dégradé :
  - ..
  - ..
  - ..
  - ..
  - ..
  - ..

Le cas échéant, éléments manquants à installer avant l'entraînement :

- ..
- ..
- ..
- ..

- Quels sont les objectifs recherchés par l'encadrement et la DSN ?
  - ....
  - ...
  - ...
  - ...
- Quels seraient les éléments probants de scénario à tester ?
  - ....
  - ...
  - ...
  - ..
  - ..

Annexe 13 : Visuel campagne cybervigilance en établissement de santé

Source : www.grand-est.ars.sante.fr/cyber-securite-en-sante

VERES	Diane	Octobre 2023

Directeur d'hôpital

Promotion 2022-2023

Cyberattaque en établissement public de santé : anticiper les conséquences de l'inéluctable

PARTENARIAT UNIVERSITAIRE :

Résumé **:**

Les cyberattaques constituent une menace majeure et avérée pour les établissements publics de santé. Nombre d'experts de la cybersécurité soulignent qu'aujourd'hui la question n'est plus de savoir si nos organisations seront cyberattaquées mais quand. Les mesures de sécurisation des systèmes d'information ne peuvent ainsi suffire à éviter ce nouveau risque. Il appartient désormais aux établissements publics de santé d'envisager la survenue d'une crise d'origine cyber afin d'organiser leur résilience.

Ce mémoire propose de redéfinir les contours de cet enjeu en précisant les modalités de survenue d'une crise d'origine cyber et en identifiant les vecteurs de vulnérabilité. Les établissements publics de santé, encouragés vers un prometteur développement du numérique en santé, doivent anticiper les conséquences de sa déstabilisation par les cybercriminels.

Fruit d'une réflexion professionnelle mêlant observation participante au CHU de Reims et témoignages de RSSI, les outils d'anticipation du risque cyber actuellement utilisés seront présentés et questionnés.

Invité à capitaliser davantage sur l'anticipation d'une crise d'origine cyber pour gagner en fiabilité, le Directeur d'hôpital pourra, au fil de ce raisonnement, s'acculturer à la technicité du risque cyber et à la prévention de ses conséquences généralisées.

Mots clés **:**

Cyberattaque – Cybersécurité – Gestion de crise – Gestion des risques – Anticipation – Fiabilité – Gouvernance – Résilience – Exercices – Simulation – Mode dégradé – Numérique – Prévention – Retour d'expérience