Directeur d'hôpital

Promotion : **2022-2023**

Date du Jury : **Octobre 2023**

La préparation des établissements de santé aux phénomènes de cyberattaques : cas du centre hospitalier Bretagne Atlantique

Laura HEURTIN

Remerciements

Mes remerciements vont tout d'abord à l'ensemble de l'équipe de direction du centre hospitalier Bretagne Atlantique (CHBA) à Vannes qui m'a accueillie en stage au sein de sa structure et qui m'a accompagnée durant ces mois d'apprentissage du métier de directeur d'hôpital. Merci tout particulièrement à ma maître de stage Marie-Dominique NAEL, directrice des projets, de la qualité et de la gestion des risques au CHBA pour son suivi, son écoute, le partage de son expérience et ses précieux conseils qui ont participé au bon déroulement de mon stage.

Merci à Olivier PLASSAIS, directeur de la transformation architecturale et digitale du groupement hospitalier de territoire Brocéliande Atlantique pour sa contribution à ce mémoire, le temps qu'il a su m'accorder, mais aussi l'intérêt et le soutien qu'il m'a apporté.

Je souhaite aussi remercier tous les agents que j'ai rencontrés et avec qui j'ai échangé et travaillé pendant mon stage, et qui m'ont fait découvrir une petite partie de leur quotidien professionnel, de leurs motivations et leur intérêt pour l'hôpital public. La diversité des profils au sein des établissements de santé est aussi challengeante qu'elle représente une réelle source d'épanouissement professionnel, de stimulation intellectuelle et relationnelle.

Enfin, merci à l'ensemble de l'équipe administrative et pédagogique de l'école des hautes études en santé publique (EHESP) pour leur implication dans notre formation et leur souhait de nous accompagner au mieux tout au long de ces deux années d'apprentissage. Un remerciement plus spécifique à Christophe VAN DER LINDE, enseignant chercheur à l'école qui m'a donné envie de choisir ce thème de mémoire et qui a été présent pour initier ce travail à mes côtés.

Sommaire

Liste des sigles utilisés

CH / CHU : Centre hospitalier / centre hospitalier universitaire
ES : Etablissement de santé
EHPAD : Etablissement d'hébergement pour personnes âgées dépendantes
GHT : Groupement hospitalier de territoire
CHBA : Centre hospitalier Bretagne Atlantique
GHBA : Groupement hospitalier Brocéliande Atlantique
RH : Ressources humaines
SI : Système d'information
DSI : Direction / Directeur des systèmes d'information
RSSI : Responsable de la sécurité des systèmes d'information
PCA / PRA : Plan de continuité d'activité / plan de reprise d'activité
RETEX : Retour d'expérience
OSE : Opérateur de service essentiel
SSE : Situation sanitaire exceptionnelle
RGPD : Règlement général sur la protection des données
DREES : Direction de la recherche, des études, de l'évaluation et des statistiques
CNIL : Commission nationale de l'informatique et des libertés
OPSSIES : Observatoire permanent de la sécurité des systèmes d'information des établissements de santé
MSS : Messagerie sécurisée de santé
CCH : Cellule de crise hospitalière
ORSAN : Organisation de la réponse du système de santé en situations sanitaires exceptionnelles
DGOS : Direction générale de l'offre de soins
ARS : Agence régionale de santé
ANS : Agence du numérique en santé
ANSSI : Agence nationale de la sécurité des systèmes d'information
ANSP : Agence nationale de Santé Publique, Santé Publique France
ANSM : Agence nationale de sécurité du médicament et des produits de santé
ABM : Agence de la biomédecine
ASN : Autorité de sûreté nucléaire
HAS : Haute Autorité de Santé
ANAES : Agence nationale d'accréditation et d'évaluation de la santé (remplacée par la HAS en 2004)

SSA : Service de santé des armées

PCME : Président de la commission médicale d'établissement

FHF : Fédération Hospitalière de France

DS : Direction / Directeur des soins

DPQGDR : Direction des projets, de la qualité et de la gestion des risques

DG : Direction Générale / Directeur Général

SDIS : Service départemental d'incendie et de secours

SAMU : Service d'aide médicale urgente

SMUR : Service mobile d'urgence et de réanimation

CESU : Centre d'enseignement des soins d'urgence

EFS : Etablissement français du sang

CDU : Commission des usagers

NRC : Nucléaire, radiologique ou chimique

Introduction

« Il n'y a que deux sortes d'entreprises, celles qui ont été attaquées et celles qui le seront » - Robert MUELLER[1]

Les 50 dernières années ont connu une accélération majeure et sans précédent des progrès numériques et technologiques. L'arrivée d'Internet a révolutionné de nombreuses activités et a transformé toutes les organisations. La quantité et le flux de données transférées sur Internet, et notre dépendance envers leur disponibilité et l'usage quotidien que nous en faisons n'a fait que croître jusqu'à aujourd'hui et la tendance n'est pas prête de s'inverser. Nous assistons à une accélération progressive du « tout informatique », bouleversant radicalement nos manières de communiquer, de consommer, de travailler... Ce monde numérique offre de nombreuses opportunités en termes d'efficience, d'évolutions technologiques, de rapidité, de possibilités diverses mais génère également de nouveaux risques. L'ampleur de la cybercriminalité est remarquable et une simple attaque de petite envergure peut réussir à compromettre l'activité d'une organisation, sa productivité, le bon fonctionnement de son système d'information, aucune n'étant aujourd'hui à l'abri des menaces cyber. En effet, les cibles des cybercriminels ne se résument pas à de grandes entreprises internationales, mais chaque individu, Etat, organisation privée ou publique, collectivité, ou toute autre organisation est menacée. Le risque cyber se définit comme « *tout ce qui touche à l'atteinte, la violation ou la perte de données, ainsi qu'à des intrusions de réseau ou à la détérioration d'actifs aussi bien matériels qu'immatériels* »[2] et se caractérise par 5 propriétés :

- Son caractère invisible
- Sa distance géographique entre le lieu de l'attaque et le lieu du sinistre
- Son caractère contagieux
- Sa dimension technologique
- La difficulté à évaluer les coûts des dégâts matériels et immatériels

Depuis quelques années, l'Etat s'est emparé du sujet de la cyber sécurité des hôpitaux en mettant en place différents programmes tel que le plan d'investissement « France 2030 » qui alloue plus de 600 millions d'euros à cet effet. Un plan blanc numérique[3] est aussi sorti en juin dernier par la DGOS afin de fournir une aide

[1] Ancien directeur du FBI (2001-2013)
[2] Définition de l'institut des actuaires, 2017 (EMERGENCE DU BESOIN EN CYBER ASSURANCE (institutdesactuaires.com))
[3] plan blanc numérique (1).pdf

méthodologique pour les établissements de santé engagés dans la mise en œuvre d'un plan de réponse aux incidents numériques et notamment des cyberattaques. Même si le volontarisme dont fait preuve en la matière l'Etat actuellement reflète qu'il s'empare réellement du problème et que des moyens sont enfin déployés pour venir en aide aux établissements, la stratégie d'anticipation a manqué et le retard accumulé dans la protection du système hospitalier face aux menaces cyber donne l'idée de l'ampleur du challenge à relever afin d'atteindre une forme de « cyber résilience ».

En effet, les établissements de santé, qu'ils soient publics ou privés, de grande ou de petite taille, sont devenus une cible qui intéresse les hackeurs. Les hôpitaux de Dax, Corbeil-Essonnes, Versailles, Villefranche-sur-Saône, Arles, Mâcon, Oloron-Sainte-Marie…. et de nombreux autres, ont été visés par des cyberattaques ces dernières années. En plein virage numérique, ces vagues successives d'attaques cyber ont paralysé une partie du système hospitalier français, forçant certains à revenir à l'ère du crayon à papier en bloquant tout ou partie de leur système d'information et donc de leur activité. En France, c'est aujourd'hui plus d'une cyberattaque à l'encontre d'un hôpital qui est enregistrée chaque semaine. Les experts en sécurité informatique de l'Agence Nationale du numérique en Santé (ANS) déplorent 730 incidents. La majorité des « rançongiciels » (technique d'attaque courante de la cybercriminalité) viendraient de groupes de hackeurs (pirates informatiques) indépendants souvent des têtes de réseau en Europe de l'Est ou d'anciennes républiques soviétiques, mais les équipes sont réparties dans le monde entier.

La cybercriminalité, qui comprend le vol, le détournement de fonds, le piratage et la destruction de données, a augmenté de 600% depuis la pandémie de Covid-19. Avec la démocratisation du cloud (serveurs informatiques à distance et hébergés sur internet pour stocker, gérer et traiter des données) et du télétravail, tous les secteurs doivent adopter de nouvelles solutions de cybersécurité, ce qui oblige autant les entreprises, les Etats et les institutions à adapter leurs techniques de travail dans l'objectif de mieux protéger leurs données.

De plus, les organisations sont confrontées à un réel manque « d'éducation cyber » de leurs salariés/agents, indépendamment de la taille de l'établissement. Ceci augmente de manière importante le risque d'accident cyber commis ou facilité par un agent : ouverture de liens provenant de destinataires suspects, mauvaise gestion du mot de passe, communication de données sensibles... Le manque de vigilance ou la méconnaissance des techniques d'attaque permettent à des pirates de récupérer des identifiants de comptes de messageries ou de déployer des rançongiciels au sein des systèmes d'information.

La préparation des établissements de santé à une meilleure maîtrise du risque cyber est longue, multiforme et nécessite une réelle prise en compte des contraintes qui pèsent

au quotidien sur le système hospitalier. Cette préparation passe par différents travaux : protection du réseau, utilisation de technologies adaptées, sensibilisation des agents, création de plans de continuité d'activité, et va jusqu'à préparer la gestion de crise elle-même avec un réel travail managérial à entamer en amont et à cultiver de façon continue.

Le sujet de la préparation des établissements de santé aux phénomènes de cyber attaque apparaît alors non seulement une thématique plus que d'actualité dans le monde hospitalier, mais représente aussi à l'heure actuelle un terrain assez vierge, peu exploité, où cohabitent bien plus de questions que de réponses.

Que représente donc concrètement la préparation au risque cyber pour un établissement de santé et quels en sont les contours ainsi que les acteurs ? Comment réaliser une préparation adaptée et complète ? Quels freins cela suppose-t-il de lever ? Et comment cultiver ce travail de préparation afin de le faire vivre ?

Tout au long de ce mémoire, nous prendrons régulièrement l'exemple du centre hospitalier Bretagne Atlantique afin d'en tirer des apprentissages en exploitant un cas récent et particulièrement intéressant de préparation au risque cyber et en tentant de rendre le propos le plus concret possible. Ce mémoire se concentrera sur une partie de la préparation des établissements, la partie managériale et de gestion de risque, sans rentrer dans les détails de la préparation plus « technique » de protection du réseau, des systèmes d'information, qui nécessite à elle seule d'être un sujet à part entière. Cette partie est d'ailleurs bien détaillée dans le plan blanc numérique de la DGOS.

Une première partie montrera que l'environnement dans lequel évoluent les établissements de santé aujourd'hui les expose à une vulnérabilité grandissante et à des risques nombreux, dont de nouveaux risques comme celui des cyberattaques. Nous verrons en quoi la lourdeur des impacts créés par la survenue d'évènements de ce type ne peut qu'obliger les établissements à s'engager dans une démarche de préparation au risque cyber.

Au sein de la deuxième partie, nous aborderons les différentes phases de cette préparation au risque cyber, passant par la sensibilisation des agents jusqu'au plan de continuité d'activité et verrons à quel point ce dernier doit être travaillé de manière opérationnelle et interdisciplinaire. Nous nous interrogerons sur la possibilité de se préparer territorialement, pour mutualiser les ressources, les compétences, et éviter que l'hétérogénéité des préparations soit biaisée par la taille ou le niveau de ressources de l'établissement.

Pour terminer ce mémoire, nous ferons un focus sur un sujet que j'ai eu l'opportunité d'explorer pendant le stage hospitalier et qui à mon sens conditionne non seulement l'efficacité d'une préparation au risque cyber mais aussi toute préparation à la gestion de risques de manière générale : l'acculturation diffuse au sein de l'établissement à la politique de gestion des risques et au management de crise.

Méthodologie

1) Contexte et choix de la thématique

J'ai réalisé une grande partie de mon stage de direction au sein de la direction des projets, de la qualité et de la gestion des risques du centre hospitalier Bretagne Atlantique où j'ai travaillé majoritairement sur le sujet des plans de continuité d'activité (PCA) de l'établissement dans le cas des risques de coupure d'alimentation électrique, d'incendie ou encore de cyberattaque. Le sujet de la préparation des établissements de santé à la gestion de divers risques a donc ponctué mon stage et m'a permis de prendre conscience des nombreuses difficultés liées à la gestion de projet à l'hôpital de manière générale, mais aussi et surtout à la difficulté de faire avancer ce type de projet, souvent considéré comme des sujets remis à plus tard car moins prioritaires.

J'ai trouvé aussi très formateur le fait de concevoir ces plans de continuité en lien étroit avec le terrain, avec chaque service de l'hôpital afin d'obtenir quelque chose de concret et d'opérationnel. Cela m'a permis de toucher à de nombreux sujets, pour certains très techniques, pour d'autres plus transversaux, mais aussi de travailler ces sujets avec des professionnels plus ou moins sensibilisés, m'obligeant à travailler sur la partie communication projet, point indispensable dans une gestion de projet.

Le fait d'avoir eu des missions ayant beaucoup tourné autour des PCA m'a donc orienté vers un choix de thématique en lien avec mon travail et donc autour de la préparation des établissements de santé à la gestion des risques. J'ai aussi trouvé indispensable le fait d'avoir pu travailler sur ce sujet, me permettant de dégager un certain nombre de points clés, de prises de recul, d'apprentissages divers qui donneront je l'espère du relief au mémoire et qui permettront d'illustrer les différents apports que j'ai tirés de ce stage.

De plus, mon stage au CHBA s'est effectué d'une part durant une période ponctuée de diverses typologies de crises que l'établissement a traversé (sortie de période covid, panne électrique, cyberattaque), et d'autre part dans une période où l'établissement a

réalisé plusieurs exercices de gestion de crise (attentat dans la ville de Vannes, rupture d'alimentation en eau, cyberattaque). Ceci a donc été pour moi une forme d'opportunité pour découvrir en tant qu'observateur la manière dont l'hôpital a géré chaque crise, mais aussi les leçons qu'ils en ont tiré à chaque fois et tous les impacts directs et indirects que cela a eu sur l'activité de l'hôpital. Le choix de cette thématique générale des « crises » en établissement de santé m'a donc paru évident, couplé à mon travail ciblant le côté « préparation aux crises / gestion des risques ».

J'ai beaucoup travaillé sur la crise de rupture d'alimentation électrique que l'hôpital a vécue en octobre 2022 et en ai notamment effectué le retour d'expérience (RETEX) ce qui fût très formateur. J'ai appris, au-delà de tous les aspects techniques qui constituent le sujet, un ensemble d'éléments méthodologiques sur la préparation à ce risque qui serviront aussi à illustrer le propos de ce mémoire.

J'ai finalement décidé d'orienter ma thématique de mémoire sur la préparation au risque cyber car d'une part son état d'avancement en ce qui concerne le CHBA est plus abouti à l'heure actuelle, et donc plus intéressant à étudier, mais aussi car ce risque est particulièrement d'actualité pour les établissements de santé de manière générale et est plutôt considéré comme un « nouveau risque » auquel les hôpitaux ne sont pas assez préparés. Ces dernières années ont vu bondir le nombre de cyberattaques des établissements de santé, qui est un sujet plutôt médiatisé et qui intéresse de plus en plus.

2) <u>Choix de la technique d'enquête :</u>

Le choix de l'entretien a été rapidement fait pour cette enquête. En effet, il s'agissait de se questionner sur le « comment » avec des informations qualitatives bien plus que quantitatives et la nécessité d'une possibilité permanente de déplacement du questionnement. Un nombre réduit d'enquêtés avec des enquêtes de temps long (environ deux heures par entretien) suffisaient à alimenter le propos et creuser différentes problématiques afin de faire ressortir différents points « fil rouge » du dossier.

Les entretiens ont été complétés par un nombre important d'échanges informels avec une variété de professionnels (encadrement, soignants, médecins) ainsi que des observations multiples avec prises de notes.

Des formes de « journaux de terrains » ont été rédigés lors des différents exercices de crise, en cellule de crise hospitalière notamment, et ont permis d'ajouter un certain nombre d'éléments plus subtils.

3) Les entretiens réalisés :

Un guide d'entretien a été réalisé afin de permettre de passer l'ensemble du sujet en revue et de n'oublier aucun point. 18 questions ont été choisies, réparties en 3 catégories (vécu de la cyberattaque, préparation au risque cyber, autres). L'idée était de lancer la conversation sur le sujet et d'avoir de nombreux fils à tirer permettant de rebondir progressivement dans un sens ou dans l'autre en fonction des profils des personnes répondant à l'entretien et de finir par aborder chaque recoin du sujet. Le nombre important de questions n'a pas fait peur aux répondants qui se sont à mon agréable surprise prêtés au jeu jusqu'au bout en ayant l'envie de répondre à chacune d'entre elles.

Il a été intéressant de découvrir l'hétérogénéité dans la sensibilisation aux différentes questions, mêlée à une forme d'homogénéité dans les réponses.

En termes de population cible pour les entretiens, et afin de compléter les prises d'informations moins formelles d'agents de l'hôpital, le personnel de direction a été le premier ciblé, aux côtés des professionnels ayant concouru de manière directe au travail de préparation au risque cyber à l'échelle de l'établissement.

Professionnels ayant répondu à l'entretien :

- **Philippe COUTURIER**, Directeur Général au centre hospitalier Bretagne Atlantique
- **Valérie JOUVET**, Directrice Générale Adjointe du centre hospitalier Bretagne Atlantique
- **Marie-Dominique NAEL**, Directrice des projets, de la qualité et de la gestion des risques au centre hospitalier Bretagne Atlantique
- **Olivier PLASSAIS**, Directeur de la transformation architecturale et digitale du GHT Brocéliande Atlantique
- **Christine ALANIC**, Responsable de la sécurité des systèmes d'informations (RSSI)
- **Stéphane LE LIMOUZIN,** Médecin coordonnateur de la gestion des risques associés aux soins
- **Séverine TECHER**, Cadre supérieure de santé – Process critique et qualité
- **Morgan MOREL**, Attaché d'administration hospitalière – Responsable de l'accueil, du standard et de l'état civil au CHBA, ainsi que du secrétariat des EHPAD, des relations avec les associations – Médiateur non médical à la commission des usagers (CDU)

Présentation du centre hospitalier Bretagne Atlantique :

Le Centre Hospitalier Bretagne Atlantique (CHBA) est le centre hospitalier de référence du territoire de santé n°4 de la région Bretagne. Il dispose de 1 419 lits et places, et emploie plus de 3 000 agents. Il dispose d'un service d'accueil des urgences 24/24, d'un Service Mobile d'Urgence et de Réanimation (SMUR) et est siège du SAMU 56, centre départemental de réception et de régulation des appels de l'aide médicale d'urgence et de la permanence des soins, ainsi que du Centre d'Enseignement des Soins d'Urgence (CESU). L'établissement situé sur 2 sites (Vannes et Auray) est en direction commune avec l'hôpital de Ploërmel, Josselin, Malestroit, Belle-Île-en-mer ainsi que l'EHPAD de Quiberon. Il est l'établissement support du Groupement Hospitalier Brocéliande Atlantique

1 Les établissements de santé évoluent dans un contexte de vulnérabilité grandissante, exposés à des risques de plus en plus nombreux et aux impacts considérables, comme celui des attaques cyber

L'environnement dans lequel évoluent les établissements de santé est en mutation constante et composé de risques divers qui rendent les hôpitaux particulièrement vulnérables et dépendants (1.1). De nouveaux risques sont aussi apparus dans le paysage hospitalier comme le risque de cyberattaque qui est particulièrement élevé aujourd'hui (1.2) et dont découlent des impacts sérieux et non négligeables pour les établissements de santé (1.3).

1.1 Les établissements de santé sont de plus en plus vulnérables et dépendants

1.1.1 Les établissements de santé sont soumis à une vulnérabilité protéiforme qui les fragilise

Les établissements de santé sont soumis à un ensemble de risques, divisés entre les risques endogènes, c'est-à-dire liés à un incident interne ou une défaillance du fonctionnement de la structure elle-même (incendie, panne électrique, rupture d'approvisionnement…), et les risques exogènes, liés à l'environnement extérieur (attentas, catastrophes naturelles, épidémies...). Les risques et les menaces ont évolué durant ces dernières années (menace terroriste, risques infectieux émergents et épidémiques, enjeux climatiques, etc.). Ces différents risques, évènements, sont générateurs de tensions hospitalières (afflux massif de patients, fragilisation du fonctionnement des structures d'accueil des urgences, carence de lits d'aval…) et mettent en difficulté les établissements de santé, en compromettant la continuité de leur activité.

La France a été ces dernières années durement touchée par des crises de natures variées (actes terroristes, risques infectieux, industriels, évènements climatiques, accidents...) et les établissements de santé ont dû répondre de manière réactive et efficace face à ces situations sanitaires exceptionnelles (SSE). Une SSE s'entend comme « la survenue d'un événement émergent, inhabituel et/ou méconnu, qui dépasse le cadre de la gestion courante des alertes, au regard de son ampleur, de sa gravité (en termes notamment d'impact sur la santé des populations ou de fonctionnement du système de

santé) ou de son caractère médiatique (avéré ou potentiel) et pouvant évoluer jusqu'à la crise[4] ». La catastrophe industrielle de l'usine AZF à Toulouse en 2001, la canicule de 2003, la pandémie grippale H1N1 en 2009, les attentats terroristes de novembre 2015, de Nice en 2016 en sont autant d'exemples. Ces situations sanitaires exceptionnelles se caractérisent par une mise en tension du système de soins, soit du fait d'une augmentation des besoins (afflux de victimes sur une période plus ou moins longue), soit d'une diminution des moyens de soins disponibles (crise dans l'hôpital)[5].

Chaque établissement de santé (ES) doit se doter d'un dispositif de crise révisé chaque année : le plan blanc. Ce dernier lui permet de mobiliser immédiatement les moyens de toute nature dont il dispose en cas d'afflux de patients, ou pour faire face à une SSE. Il intègre les orientations du dispositif d'organisation de la réponse du système de santé en situations sanitaires exceptionnelles (ORSAN), déclenché par le préfet en articulation avec l'ARS, qui définit les parcours de soins des patients coordonnés et adaptés aux événements au niveau régional. La création du dispositif ORSAN permet aux ARS de mobiliser l'ensemble des secteurs de l'offre de soins face aux SSE. Le dispositif ORSAN comprend les 5 volets suivants :

- ORSAN AMAVI : accueil massif de victimes d'un évènement grave (accident, catastrophe, attentat)
- ORSAN EPI CLIM : prise en charge des tensions dans l'offre de soins liées au nombre important de patients dans un contexte d'épidémie saisonnière et/ou lors d'un phénomène climatique voir environnemental important
- ORSAN REB : prise en charge des patients dans le cadre du risque épidémique et biologique connu ou émergent
- ORSAN NRC : prise en charge des patients dans le cadre d'un évènement nucléaire, radiologique ou chimique
- ORSAN MEDICO-PSY : prise en charge médico-psychologique des patients victimes d'un évènement grave

Chaque établissement doit disposer d'un plan global de gestion de crise, complètement intégré dans sa gouvernance. Cette organisation interne et structurée doit prendre en compte l'ensemble des risques auxquels il peut être confronté. L'organisation autour des SSE, s'appuie sur un guide[6], visant à proposer un cadre actualisé de préparation

[4] 1 (sante.gouv.fr)
[5] 64-ch55-715-724-9782294769580 (ce-mir.fr)
[6] Guide de gestion des tensions hospitalières et des situations sanitaires exceptionnelles au sein des établissements de santé - Ministère de la Santé et de la Prévention (sante.gouv.fr)

et de gestion de crise, en cohérence avec les procédures de mobilisation des ressources sanitaires locales, régionales et nationales.

La gestion des SSE s'inscrit dans un cadre défini faisant intervenir différentes autorités et structures compétentes. 4 échelons peuvent être mobilisés :

- Le niveau national : ministère en charge de la santé avec appui des agences sanitaires (ASN, ANSP, ANSM, EFS, ABM..), ministère de l'intérieur, ministère des armées (SSA), autres ministères
- Le niveau zonal : préfet de zone, ARS de zone, SAMU zonal
- Le niveau régional : ARS
- Le niveau départemental : préfet de département, SAMU, SDIS et associations agréées de sécurité civile

De plus, d'autres problématiques diverses se sont accumulées ces dernières années à l'hôpital public, sans avoir trouvé aujourd'hui de solution suffisante, ceci venant aggraver les conditions des établissements de santé et leur capacité à exercer correctement leur activité. Les problématiques d'attractivité de nombreux métiers de l'hôpital induisent d'importantes difficultés de recrutement. D'après une étude[7] publiée au printemps 2022 par la Fédération hospitalière de France (FHF), la quasi-totalité des hôpitaux (99%) connaît des difficultés de recrutement, de manière permanente ou ponctuelle, selon les remontées de 400 établissements. Ce phénomène ayant pour conséquence « la hausse de la fatigue des soignants » (90% des établissements) et la « hausse du recours aux heures supplémentaires et du recours à l'intérim » (67% des établissements).

Plus globalement, l'hôpital absorbe toutes les évolutions sociétales et sociologiques et ne peut en l'état trouver de solutions à des problématiques bien plus larges et complexes que sa seule organisation, ce qui explique qu'il finit par les subir et se fragilise. Les aspirations professionnelles et personnelles des nouvelles générations ont changé, notamment en termes de qualité de vie au travail et les établissements doivent s'adapter. Ces nouveaux challenges représentant autant d'opportunités que de contraintes à l'heure actuelle, et peuvent mettre les établissements de santé dans des situations de tensions.
L'hôpital est donc devenu une organisation en situation de crise permanente, la gestion de l'urgence étant le quotidien des professionnels. La crise Covid a accéléré ce phénomène et a fortement impacté les conditions de travail à l'hôpital alors que le secteur hospitalier était déjà connu pour ses difficultés. D'après une étude de la DREES de juillet 2022[8], 1

[7] Enquete RH 2022 synthèse_2006.pdf (fhf.fr)
[8] er1235_0.pdf (solidarites-sante.gouv.fr)

personne sur 2 a travaillé dans des services principalement dédiés à la prise en charge du Covid-19 (« services Covid ») entre mars 2020 et l'été 2021, que ce soit de façon continue ou durant certaines périodes. Parmi ces dernières, 2 sur 3 ont connu des périodes inhabituelles de surcharge de travail. Les restrictions de visites ont eu un impact sur l'augmentation de l'accompagnement nécessaire de la part des patients. Parmi les agents ayant travaillé dans un service Covid, 1 sur 2 a craint que sa santé ne soit mise en danger par ses conditions de travail et 8 sur 10 ne ressentent pas plus de reconnaissance envers leur travail qu'avant la crise.
France Assos Santé confirme cette dégradation générale dans une enquête dévoilée en octobre 2022[9] sur la crise de l'hôpital, réalisée auprès de 655 patients et représentants d'usagers témoignant d'une « dégradation de l'offre avec un retard ou un report des soins ainsi qu'une détérioration du lien soignant/soigné ». Le constat est unanime.

Nous verrons par la suite toutes les difficultés que cette « gestion permanente de l'urgence » a pour conséquences et les freins que cela pose pour pouvoir faire avancer des projets transversaux, considérés moins prioritaires car moins urgents.

L'enjeu pour les établissements de santé est aujourd'hui de poursuivre ses activités malgré les menaces endogènes et exogènes qui pèsent sur lui, tout en ayant des objectifs de plus en plus exigeants en termes de qualité et de sécurité des soins.

1.1.2 Les établissements de santé sont d'autant plus vulnérables qu'ils sont devenus ultra dépendants

Les diverses évolutions qu'a connu l'hôpital ces dernières années l'ont rendu ultra dépendant, que ce soit aux énergies (eau, gaz, électricité…) ou aux technologies informatiques et de communication notamment. Ce niveau de dépendance s'est vu croître bien plus rapidement que le niveau de maîtrise de cette même dépendance, et place donc les hôpitaux aujourd'hui dans une position de faiblesse vis-à-vis de leur ultra dépendance qu'il ne savent à l'heure actuelle pas maîtriser.

Si l'on prend l'exemple de l'électricité, l'ensemble des services des établissements de santé en ont besoin pour fonctionner et peuvent se retrouver paralysés à l'occasion d'une rupture d'alimentation. Absolument toutes les activités présentes à l'hôpital ont besoin d'électricité : éclairage des locaux, accès aux locaux via ascenseurs, chauffage/climatisation/ventilation/traitement d'air, sécurité via les portes automatiques/à codes/à badge, appels-malades, matériel de surveillance et télésurveillance patient

[9] Crise de l'hôpital : A leur tour, les patients témoignent d'une situation critique ! - France Assos Santé (france-assos-sante.org)

(tensiomètres, saturomètres, appareils à ECG, scopes,…), informatique pour l'accès au dossier patient, aux traitements, aux prescriptions,… la liste est presque illimitée. Certains services, identifiés comme faisant partie de la plaque tournante de l'hôpital, (services d'imagerie, laboratoire, pharmacie) peuvent aller jusqu'à paralyser l'ensemble de l'établissement s'ils ne disposent plus d'électricité. Dans le cadre d'un établissement de soins, accueillant des personnes vulnérables, le risque est d'autant plus élevé que l'impact peut être maximal en termes de continuité des soins allant de la simple désorganisation du service jusqu'à la perte de chance notoire, voire le décès d'un patient.

Notons aussi un autre impact lié à cette dépendance à l'énergie : l'impact financier pour le budget des hôpitaux, ce dernier ayant flambé à cause de l'inflation et creusant le déficit de bon nombres d'établissements, fragilisant leur « santé financière ».

Même si cette dépendance multiple peut paraître logique et inévitable au vu des évolutions des dernières années, les établissements ne peuvent en prendre conscience que dans le cas où ils en sont littéralement privés ou bien s'ils décident d'entamer un travail de préparation au risque en question. C'est exactement ce qu'il s'est passé dans le cas du CHBA lors de sa préparation aux risques de cyberattaque et de coupure d'alimentation électrique. Dans les deux cas, en travaillant les impacts service par service et les solutions dégradées à mettre en place, les professionnels ont commencé à réaliser l'ampleur de cette dépendance, qui peut d'ailleurs paraître effrayante, particulièrement quand elle n'est pas du tout maîtrisée. Le constat des personnes interrogées dans le cadre de l'enquête de ce mémoire a d'ailleurs été unanime sur ce point. Les impacts d'une cyberattaque ou d'une coupure électrique sont lourds et diffus, et le fait d'y être confronté permet d'en apprécier la réalité.

Une des grandes dépendances des établissements de santé, ou de toute organisation de manière générale, est aussi l'informatique ainsi que la téléphonie. Concernant la téléphonie, y est rattaché le premier moyen de communication qui existe à l'hôpital, permettant au-delà des communications quotidiennes interservices le fonctionnement des astreintes médicales, des urgences vitales… Faire fonctionner l'hôpital sans téléphonie du jour au lendemain paraît presque inenvisageable, et pourtant, une cyberattaque peut avoir pour conséquence la perte de la téléphonie au sein de l'établissement.

Concernant le numérique, il a bouleversé les usages à l'hôpital et a permis d'améliorer l'efficience du système de soins tant pour les patients que pour les professionnels. La feuille

de route[10] 2023 – 2027 du numérique en santé lancée en mai 2023 confirme les ambitions du national de mettre le numérique encore plus au cœur de notre système de santé. L'avenir des hôpitaux sera donc toujours numérique-dépendant et les conséquences d'une perte d'accès au numérique seront encore plus lourdes. En effet, l'activité de chaque service de l'hôpital est conditionnée à l'utilisation de ses différents logiciels métiers, sans lesquels toute l'organisation doit être repensée via des « procédures dégradées » plus ou moins opérationnelles. Prenons l'exemple du laboratoire du centre hospitalier Bretagne Atlantique réalisant environ 2000 analyses quotidiennement en temps normal et seulement une centaine en procédure dégradée. L'impact est énorme, d'une part pour l'ensemble de l'établissement mais aussi pour ses partenaires extérieurs, avec qui il va devoir collaborer pour subvenir à la demande.

1.2 Le risque de cyber attaque est aujourd'hui plus élevé que jamais

1.2.1 La vague de cyberattaques de ces dernières années réveille progressivement les consciences

D'après le guide plan blanc numérique de la DGOS, les incidents numériques et notamment les cyberattaques se sont récemment multipliés sur les établissements de santé. Les signalements ont, dans le secteur de la santé, doublé en 2021 par rapport à 2019 et 2020.

« *La question n'est pas de savoir si cela va arriver, mais* quand » a résumé Guillaume Guiguené, ingénieur chez OneTrust (société de gestion des risques et de protection des données de santé) à la conférence du Forum international sur la cybersécurité intitulée "Hôpitaux : comment renforcer la préparation en cybersécurité ?" ayant eu lieu le 24 janvier 2023. Il y a été souligné le manque important de nombreux hôpitaux au risque cyber, et la nécessité d'un changement de culture.

Le dernier rapport[11] de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a notamment relevé que les hôpitaux figurent à la troisième place des cibles privilégiées des pirates (10% des rançongiciels traités/rapportés à l'ANSSI en 2022), derrière les PME, TPE et ETI (40%) et les collectivités territoriales (23%). D'après Vincent Trely, président-fondateur de l'APSSIS (association pour la sécurité des systèmes de

[10] Concertations du numérique en santé - Feuille de route du numérique en santé 2023 - 2027 - Présentation (esante.gouv.fr)
[11] L'ANSSI PUBLIE SON RAPPORT D'ACTIVITÉ 2022 : UNE ANNÉE DENSE POUR ASSURER UNE RÉSILIENCE CYBER DE PREMIER PLAN | Agence nationale de la sécurité des systèmes d'information

santé), « *il n'y a pas de volonté spécifique des pirates de s'en prendre aux établissements de santé* », ces derniers représenteraient une « *cible facile, où des dizaines de postes fonctionnent sous Windows XP, des appareils médicaux achetés dans les années 90 ou 2000…* ».

En février 2019, le CHU de Rouen s'est fait cyberattaqué. En 2021, ce sont au tour des CH de Dax et de Villefranche-sur-Saône, en 2022 l'hôpital de Vitry-le-François victime d'un vol massif de données, l'hôpital de Corbeil-Essonnes touché par une cyberattaque rendant impossible tous les examens nécessitant les moyens informatiques, l'EHPAD Les Franches Terres à Beuzeville ayant subi un cryptage de données, mais aussi le CH de Versailles. Le groupe ELSAN a de même été attaqué en 2022, et rien que sur la région Bretagne, les CHU de Rennes et de Brest ont récemment subi une cyberattaque, ainsi que la clinique Saint-Laurent. Les exemples sont de plus en plus nombreux, et le chronogramme technique est toujours le même : fermer tous les accès internet, empêchant l'exfiltration de données et limitant drastiquement les impacts qui suivent. Certains établissements de santé ont mis énormément de temps à se remettre de l'attaque. Les CH de Dax et de Versailles en sont un bon exemple, ils ont été en très grande difficulté pour maintenir la prise en charge de leurs patients. A l'hôpital de Dax, plus de la moitié des équipements informatiques ne sont pas encore réparés. Toutes les données patients ont été perdues, ce qui a obligé l'hôpital à tout réenregistrer, et les différents programmes ne sont pas tous revenus à leur mode de fonctionnement normal, *"Il faut quatre heures pour une demande d'examen de biologie, contre 45 minutes auparavant",* déplore Vincent Trely, président-fondateur de l'APSSIS (association pour la sécurité des systèmes d'information de santé).

Une recrudescence sans précédent d'attaques par rançongiciel couplée à une évolution importante des cyberattaquants met aujourd'hui le risque cyber au premier plan pour les établissements de santé. Le profil des hackeurs a changé, passant d'hackeurs individuels ou de petits groupes à un écosystème complexe et varié d'acteurs ayant des outils plus développés et plus puissants.

Les établissements de santé sont la cible de différents types de menaces :

- Le ransomware ou rançongiciel : menace utilisée par les hackeurs du CH de Dax et de Corbeil-Essonnes. Logiciel malveillant bloquant l'accès aux ordinateurs et données personnelles tant qu'une rançon n'a pas été versée. Une fois infiltré, le rançongiciel se propage dans tout le SI et crypte les données les rendant inexploitables. La rançon est demandée en échange d'une clé de déchiffrement, cependant le paiement de rançon est interdit afin de ne pas multiplier les attaques. Le dépôt de plainte lui doit être automatique.

- Le Phishing ou hammeçonnage : Attaque visant à obtenir des données via l'usurpation d'identité, les hackeurs se faisant passer pour des entités connues (banques, opérateur téléphonique, autres…).
- Spearphishing ou fraude au président : basée sur une usurpation d'identité plus ciblée

La prise de conscience autour du risque de cyberattaque chez les établissements de santé est difficile à évaluer. Ce risque paraissait jusqu'alors à priori « peu probable », mais le nombre grandissant d'établissements cyberattaqués, couplé à une communication importante dans la presse alerte progressivement de plus en plus d'établissements, de grande taille comme des CHU, mais aussi de bien plus petite taille comme des établissements médico-sociaux autonomes. La prise de conscience de la part des établissements de leur vulnérabilité n'engage cependant pas obligatoirement de démarche de sécurisation et de protection face au risque car même s'il est réel, il n'en est pas moins secondaire face aux autres obligations et contraintes qui leur incombent. « *Nous savions que nous devions le faire, cela avait été identifié dans le programme de travail* », « *notre niveau de préparation était cependant très faible, si ce n'est inexistant…* », « *je ne pense pas que les établissements de santé soient conscients de leur vulnérabilité, il faut malheureusement vivre une cyberattaque pour l'objectiver* » (M-D NAEL, CHBA).

La sensibilité aléatoire des directeurs généraux d'établissements créé elle aussi des disparités dans les niveaux de préparation de chacun.

Depuis la première cyberattaque ayant eu lieu sur un établissement de santé de grande taille, le CHU de Rouen en 2019, les établissements ont tout de même commencé à s'adapter en répartissant les données de façon à ne pas tout perdre en cas d'attaque cyber ou en prévoyant un certain nombre de sauvegardes. Cependant c'est un changement de culture qui fera la différence d'après André Zaphiratos (Directeur des systèmes d'information de la Fondation Cognacq-Jay, œuvrant dans la solidarité sociale) « *A chaque fois, des erreurs humaines sont à la base de défaillances* ».

Dans son rapport annuel, l'ANSSI regrettait « *des faiblesses dans la sécurisation des données, des usages numériques non maîtrisés, ainsi que le manque d'allant des organisations qui même prévenues de la menace, ne se sont pas adaptées* ».

1.2.2 Les établissements de santé, une nouvelle cible pour les hackeurs

Le 7 décembre dernier, au CHBA, l'annonce par les agences d'état d'une intrusion et d'une exfiltration des données a été un électrochoc. Une cellule de crise institutionnelle a été mobilisée dans l'urgence, ainsi qu'une cellule de crise opérationnelle. La répartition des rôles a été primordiale, le RSSI était en lien avec l'ANSSI, la responsable ingénierie en lien avec Orange cyber Défense, et le Directeur des systèmes d'information en cellule de crise avec une communication asynchrone entre sa cellule opérationnelle et la cellule de crise permettant d'avoir les informations et l'évolution de la situation en temps réel.

Le 8 décembre, début de la phase d'investigation aux côtés du Cert-Santé et d'Orange Cyber Défense en lien étroit avec l'ANSSI. A partir du 8 décembre et jusqu'au 15 décembre, 2 points par jour ont été effectués avec le Cert Santé, tenue d'une main courante, communication de l'avancée des investigations au DSIT, échange avec la police suite au signalement. Le 15 décembre, le Cert-Santé rend son rapport, fin de la phase d'investigation :

- Exfiltration d'environ 100 Mo de données sans connaissance du contenu des données exfiltrées
- Pas d'impact sur les autres établissements
- Passage vers la phase de remédiation

Le CERT impose de communiquer sur l'évènement. Le CHBA a fait le choix de communiquer de manière anonyme. Le support a été proposé par le CERT et amendé par le RSSI.

Du 9 janvier jusqu'à mi-mai a lieu la phase de remédiation :

- Contractualisation avec un PRIS (Prestataire de Réponse à Incident de Sécurité), Orange Cyber Défense (OCD)
- Accompagnement de la part des experts (mise en conformité avec les bonnes pratiques. La cible consiste à atteindre un niveau donné par un outil d'audit).
- Sur les premières semaines :
    - 2 personnes d'OCD sont présentes au CHBA
    - Point hebdomadaire a lieu les premières semaines : RSSI – responsable Ingénierie - OCD
    - Point quotidien a lieu : OCD – Responsable ingénierie – équipe système

En parallèle :

- La direction des soins constitue des caisses cyber : contribution de l'équipe support de la DSIT
- Constitution d'un annuaire des GSM de secours : contribution de l'équipe réseau télécom

- Ordinateurs mis à disposition dans tous les services pour accéder à Internet de manière autonome et minimiser l'impact

L'ouverture des accès Internet imposait que les actions de remédiation soient conduites au risque de se faire réinfiltrer ce qui a représenté une forte pression sur la durée. Les utilisateurs ont bien compris la mesure dans les premières semaines, cependant il a été plus difficile de le faire comprendre sur plusieurs mois. L'évènement Cyber a permis à l'établissement de faire un immense saut en terme de PCA qui n'aurait jamais été possible avant, mais également en termes de sécurité (accès distant au SI).
Cela a donc été une réelle opportunité pour l'établissement. Il est désormais plus facile de porter un message/des actions sur la sécurité des SI. Le constat a aussi été fait que les utilisateurs ne maîtrisent pas du tout l'informatique (ne savent pas accéder à un site s'il n'y a pas de moteur de recherche, des ordinateurs autonomes étaient mis à disposition pour les accès internet. Les utilisateurs avaient du mal à les exploiter).

La décision de couper tous les accès internet a été prise une heure après l'alerte sans connaître réellement les impacts (télétravail, télé suivi des patients..). Le premier enjeu était en effet de stopper toute attaque ou exfiltration de données. L'établissement s'est immédiatement mis en position de gestion de crise en lien direct et constant avec l'ANSSI. Le second enjeu a été de redonner accès aux sites internet stratégiques pour les professionnels. Le CERT-Santé et l'ANSSI ont accompagné le CHBA pendant de longues semaines avec efficacité. En parallèle, les services ont travaillé sur leur PCA.

Quand on demande aux différents professionnels de l'établissement quelles sont à leur avis les raisons du phénomène de cyberattaques sur les établissements de santé les réponses sont variées, oscillants entre une incompréhension et un manque d'éthique pour certains, la rançon et la valeur des données à la revente pour d'autres.
« La valeur des données de santé est de plus en plus importante et le niveau médiatique est très important » (O. PLASSAIS, CHBA) ; « il peut s'agir de sources de profits, de capacité de chantage » (M-D. NAEL, CHBA) ; « cela paraît irréaliste et assez incompréhensible, quel est l'intérêt ? et éthiquement ? je n'en comprends pas le sens », « nous avons néanmoins tout un ensemble de données qui peuvent peut-être se revendre sur le darknet… il y a aussi la rançon… » (V. JOUVET, CHBA) ; « la valeur des données patients, réelle ou symbolique ? le chantage aux établissements avec les rançons, la compétition de reconnaissance entre les hackeurs, les hôpitaux pouvant être considérés comme des trophées » (P. COUTURIER, CHBA) ; « la revente des données des patients et des professionnels » (M. MOREL, CHBA)

Les établissements de santé ont vu leur vulnérabilité au risque cyber augmenter ces dernières années pour plusieurs raisons. L'agence nationale de la sécurité des systèmes d'information (ANSSI) évoque l'absence de maîtrise des systèmes d'information, le manque de sensibilisation aux risques cyber et le non-respect des bonnes pratiques du numérique, l'augmentation de la surface d'attaque due aux pratiques de télétravail ainsi que le manque de professionnels experts en cyber sécurité au sein des établissements.

Les hôpitaux ont été une cible privilégiée des attaques cyber lors de l'épidémie de Covid 19, l'ancien président de la FHF Frédéric Valletoux explique ce phénomène : « *On doit estimer que ce sont des proies faciles, qu'ils ont la tête ailleurs, qu'ils sont mobilisés par l'épidémie, la prise en charge des patients, par une activité débordante et que peut-être l'attention diminue quant aux précautions à avoir en matière de sécurité informatique* ». Ces propos sont en accord avec ceux de l'APSSIS (l'association pour la sécurité des systèmes d'information de santé) datant de juin 2020 : « *Le coronavirus semble avoir largement inspiré les cybercriminels puisque le baromètre Signal Spam indique que le phishing aurait augmenté de 600 % sur le mois de mars* ». La crise sanitaire aurait donc aussi accentué le risque de cyberattaques pour les établissements de santé dû à une position de vulnérabilité pouvant être exploitée par les cybercriminels.

D'après l'entreprise Crysalide (société de conseil aux entreprises spécialisée dans les risques cyber), différentes raisons expliquent cette augmentation des cyberattaques visant les établissements de santé. Les hôpitaux seraient « *plus susceptibles de céder aux demandes de rançon* » afin de retrouver l'accès à leurs infrastructures critiques et aux données patients qui sont des données hautement sensibles. De plus, les hôpitaux étant des acteurs essentiels, très dépendants du numérique : la rupture des systèmes d'information met en péril la continuité et la qualité des soins, la logistique... les conséquences peuvent être désastreuses. Les établissements de santé souffrant aussi d'un manque d'investissement dans la sécurisation de leurs systèmes informatiques, cela les rend plus vulnérables. Les logiciels sont souvent anciens et les mises à jour ne figurent pas toujours dans les priorités de la structure. Enfin, les erreurs humaines comme l'ouverture de pièces jointes sont potentiellement plus fréquentes dans le contexte de stress et d'urgence de l'hôpital, diminuant la vigilance du personnel.

Les établissements de santé sont cependant loin d'être les seules organisations à être cyberattaquées. Des entreprises, des collectivités, sont cyberattaquées partout dans le monde, personne ne semble épargné par les cyber menaces, du plus petit au plus grand. En ce sens, un plan de lutte contre la cybercriminalité d'un milliard d'euros a été annoncé par Emmanuel Macron le 18 février 2021. Ce dernier a pour objectif d'être appliqué d'ici 2025 et comprend 5 axes :

- Le développement de solutions nationales de cyber sécurité et l'augmentation du chiffre d'affaires de ce secteur
- Le renforcement des liens et synergies entre les acteurs de la cyber sécurité
- La mise en place des actions de sensibilisation pour promouvoir les solutions nationales
- Le soutien en fonds propres dédié aux startups
- Le renforcement d'un volet formation dans le but de doubler les emplois de la filière afin de passer de 37 000 à 75 000 postes

Les enjeux sont les suivants :

- Améliorer l'interopérabilité entre les applications utilisées quotidiennement par les établissements de santé
- Mettre en place et encadrer le développement de toutes les activités à distance (toutes les formes de télémédecine, télétravail) grâce à des applications sécurisées
- Intégrer une solution de sécurisation de messagerie, l'email représentant le vecteur principal d'attaque

De plus, les 137 GHT ont intégré la liste des opérateurs de service essentiels (OSE) afin de les contraindre à appliquer les meilleures pratiques de cybersécurité aux SI actuels mais aussi d'apporter des règles de sécurité informatique plus strictes. Le contrôle du respect de ces règles sera du ressort de l'ANSSI et les ARS devront accompagner les différents GHT de leurs régions dans leur mise en conformité avec ces mesures.

1.3 La diversité et la lourdeur des impacts d'une cyberattaque apparaissent non négligeables pour les établissements de santé

1.3.1 Des impacts majeurs en termes de continuité d'activité et de sécurité des soins

Au regard de l'impact d'un incident numérique sur un établissement de santé, l'organisation des soins en mode dégradé doit être travaillée. Les impacts peuvent en effet être nombreux et lourds, affectant des services et activités essentiels de l'hôpital. Le réseau téléphonique et la messagerie peuvent être rendus inaccessibles, d'où l'importance de formaliser un plan de continuité d'activité. Une cyberattaque peut se traduire par l'impossibilité pour le personnel soignant d'accéder aux dossiers des patients et donc aux prescriptions, traitements, antécédents médicaux ; ainsi que l'impossibilité d'effectuer des demandes d'examens (biologie, imagerie), notamment des examens d'urgence.

L'utilisation des différents logiciels et applications métiers, systèmes de stockage en imagerie peuvent aussi être rendus inaccessibles, tous ces impacts ayant pour conséquence la nécessaire déprogrammation d'actes et examens de patients. Une cyberattaque peut donc donner lieu à des répercussions nombreuses pour l'activité de l'établissement :

- Logiciels métiers non fonctionnels (laboratoire, imagerie, pharmacie…)
- Impossibilité de joindre le SAMU-Centre 15, voir indisponibilité temporaire du SAMU-Centre-15 dans le cadre d'un établissement siège du SAMU (nécessité de transférer les lignes du SAMU potentiellement vers le SDIS en première intention puis vers un des SAMU voisins, procédure à organiser)
- Planning du bloc opératoire indisponible, impossibilité de visualiser les images au bloc
- Indisponibilité des machines d'imagerie, et/ou des logiciels de lecture et d'interprétation d'imagerie
- Panne du réseau GTC (chauffage, climatisation, traitement d'air…), conséquences démultipliées en temps de canicule ou d'hiver très froid. Le traitement d'air ou la ventilation non fonctionnel rend aussi impossible certaines activités (reconstitution de poches de chimiothérapies…)
- Absence de traçabilité de l'activité de stérilisation, voire indisponibilité de fonctionnement global de l'activité entraînant des conséquences lourdes sur l'activité de bloc opératoire
- Inaccessibilité d'accès à l'historique des examens, aux comptes rendus d'examens, aux résultats de biologie
- Gestion du parcours patient perturbée (admission du patient, création d'étiquettes, sortie du patient, certificats de décès…)
- Dossier patient informatisé indisponible
- Panne du réseau téléphonique (standard de l'hôpital) et de la messagerie
- Indisponibilité de certains dispositifs médicaux connectés, de télésurveillance, d'alarmes…
- Perturbation des fonctions logistiques (gestion des repas, gestion des déchets, distribution des médicaments, service coursier)
- Perturbation de certaines fonctionnalités administratives (gestion de la paie par exemple)
- Autres impacts

La liste des potentiels impacts liés à une cyberattaque est longue et dépend aussi du fonctionnement de chaque établissement. « *Il y a des décisions lourdes à prendre en en*

cas de cyberattaque, comme quels patients doivent partir en réanimation ? », « *l'hôpital doit ensuite fonctionner de façon dégradée pendant une durée indéterminée* », « *la régulation des urgences* », « *la déprogrammation d'opérations chirurgicales dû à l'absence de fonctionnement normal des services d'imagerie et de laboratoire* », « *tout ce qui est sensible est désorganisé, cela n'a rien d'anodin pour un hôpital* » explique le président de l'APSSIS, Vincent Trely.
De plus, « *l'écart reste terrible* » entre les pratiques recommandées par l'ANSSI et celles de certains hôpitaux d'après le Directeur des systèmes d'information de la Fondation Cognacq-Jay.

Si l'on prend l'exemple du centre hospitalier de Dax, attaqué le 9 février 2021 par le ransomware Ruyk, cette cyberattaque a réussi à mettre hors service la totalité du système d'information de l'hôpital avec un coût total associé à l'attaque de 2,3 millions d'euros. Le CH de Corbeil-Essonnes a lui eu une demande de rançon de 10 millions de dollars, avec l'ultimatum suivant : l'hôpital devait payer la rançon sous un mois ou le groupe cybercriminel Lockbit divulguait une dizaine de giga-octets de données. N'ayant pas cédé à la pression, les menaces ont été mises à exécution. Cette méthode s'appelle la « double extorsion » et consiste à voler des données et faire pression sur les victimes avec la menace de divulgation de toutes ces données. Si la rançon n'est pas payée, les hackeurs peuvent se rémunérer en revendant les données de santé sur des marchés parallèles et illégaux (un dossier médical pourrait être revendu jusqu'à 300 euros).

En termes d'impacts, il y a bien évidemment tout le volet technique mais pas seulement. Nombreux sont les impacts organisationnels : le déport d'activité vers les établissements et partenaires extérieurs (c'est ici que l'hôpital se rend compte à quel point il s'inscrit dans un environnement avec de nombreux partenaires extérieurs). Il faut adapter tous les processus de prise en charge patients, dû à l'impossibilité d'avoir accès au système d'information, mettre en œuvre les processus dégradés le plus rapidement possible.
De plus, pour les professionnels, tenir ces procédures dégradées pendant 24 heures, 48 heures, 72 heures, une semaine, un mois ou un an n'a pas les mêmes conséquences. En avril 2022, le groupement hospitalier de territoire Cœur Grand Est est victime d'une attaque cyber. Ils ont eux aussi pris la décision de couper les accès, et les 9 centres hospitaliers et 5500 professionnels du groupement s'en sont retrouvés coupés d'internet. Un an plus tard, ils ont toujours du mal à retrouver une situation normale.

« Les données sont sensibles et les fuites de données patients ont un fort impact sur le public. Par ailleurs, le fait de bloquer un établissement de santé prend en otage tout un

bassin de population et l'émotion pourrait être grande en cas d'impact en termes de perte de chance ou de décès patient » (S. TECHER, CHBA). Un évènement dramatique a eu lieu à l'hôpital de Dusseldorf[12] en Allemagne alors qu'il était victime d'une cyberattaque qui paralysait le fonctionnement de ses services et a donc forcé un certain nombre de transferts de patients urgents vers d'autres établissements. Une patiente est décédée de ce transfert, faute d'avoir reçu les soins nécessaires à temps.

En effet, les impacts d'une cyberattaque sont d'autant plus lourds quand ils se combinent avec les contraintes propres au secteur hospitalier. La menace cyber qui s'exerce sur les entreprises, administrations et hôpitaux est sensiblement la même. Cependant, le monde hospitalier se distingue par son obligation de continuité d'activité. Ce dernier doit rapidement renforcer ses efforts en prenant en compte ses limites structurelles. Le budget en est l'une d'elle : alors que les entreprises consacrent en moyenne 4 à 5% de leur budget à la cybersécurité, l'hôpital n'en dédie qu'1 à 2% donc 2 à 3 fois moins. L'hôpital investit trop peu dans l'informatique et le budget est majoritairement consacré à des frais de fonctionnement.

1.3.2 Des impacts financiers, d'investissements, mais aussi psychologiques et même juridiques

Même si les impacts en termes de continuité des soins apparaissent comme les plus importants, il n'en reste pas moins qu'ils ne sont pas les seuls. L'impact financier est considérable, et peut mettre un établissement de santé en grande difficulté financière. Les impacts en termes d'image, mais aussi les impacts psychologiques pour les professionnels, ou encore juridiques pour l'établissement ne doivent pas être mis de côté.

« *Le sujet de la préparation au risque cyber est important car tous les établissements de santé n'ont pas forcément les moyens d'investir* » (M-D. NAEL, CHBA). En effet, le risque financier est conséquent : les coûts afférents, en fonction de l'ampleur des dégâts, rassemblant le rachat de matériel, les coûts d'intervention, les frais d'interruption d'activité, le manque de recettes, les investissements technologiques mais aussi tous les « nouveaux coûts » comme le recrutement de profils cyber ou la formation des agents… sont estimés à 5 à 10 fois plus élevés que le coût de la rançon.

[12] Un mort après une cyberattaque contre un hôpital allemand - Sciences et Avenir

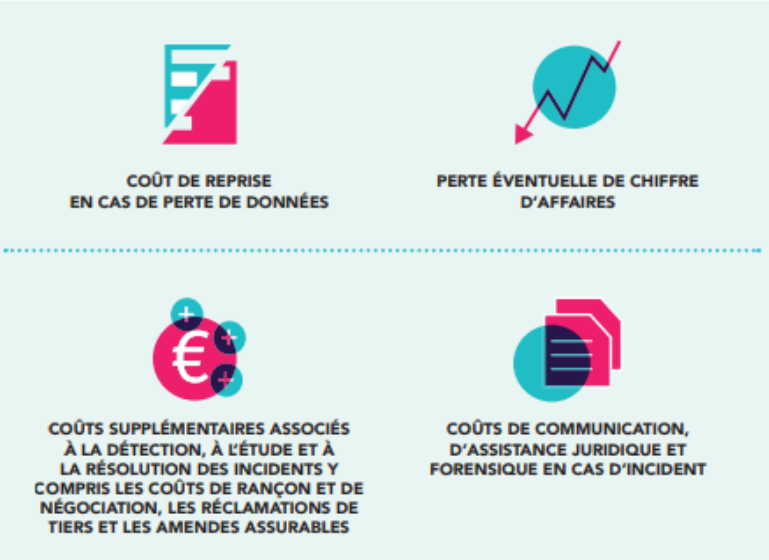
D'après Tic Santé[13], le coût total de l'attaque cyber subie par le CH de Dax en 2021 s'élève à 2,3 millions d'euros « compensés par l'ARS », information délivrée par le RSSI de l'hôpital Nicolas Terrade, lors d'un retour d'expérience effectué par le CH. Cette cyberattaque avait « *mis hors service la totalité de son SI* », le montant se décompose ainsi :

- Coûts RH, renforts et heures supplémentaires : 1,48 million d'euros
- Prestations cybersécurité et réinstallations : 546 000 euros
- Investissements (matériel reconstruction réseau) : 174 000 euros
- Pertes de recettes commerciales : 143 000 euros
- Sous-traitance biologie : 9 000 euros

Afin répondre au risque financier que représente une cyberattaque pour une organisation, la solution de l'assurance aujourd'hui commence à se poser pour les établissements de santé, même si la réflexion n'est qu'à ses prémices. En effet, il existe des assureurs proposant des contrats personnalisés contre les cyber-risques. Ils procèdent à une première analyse des risques spécifiques à l'organisation, afin de déterminer si le recours à une assurance contre les cyber-risques est nécessaire et si oui laquelle, avec le type de couverture adapté en fonction :

- Du volume de données traitées et de leur type
- Du type de réseau de distribution
- De l'exposition de l'organisation

Comme chaque contrat d'assurance, une indemnisation est versée quand un seuil est dépassé.



[13] TICsanté - Articles (ticsante.com)

Ces assurances représentent un marché à haut potentiel de croissance, se développant de la même manière que la gestion des risques cyber des organisations. Le marché de l'assurance cyber au niveau international connaît en effet une hausse ces dernières années, mais l'Europe est à la traîne et peu d'organisations ont l'habitude de conclure ce type de contrat d'assurance. Les raisons sont surement plusieurs, une sensibilisation moins forte, un risque qui jusqu'ici n'était pas assuré, une règlementation non adaptée… A ce jour, il existe peu de données sur les assurances de ce type, afin de pouvoir évaluer l'utilité de ce dispositif, notamment pour les établissements de santé.

Les professionnels et les patients peuvent devenir eux aussi de véritables dommages collatéraux. Pour les équipes, l'impact psychologique n'est lui non plus pas à négliger s'agissant d'un évènement aussi perturbant et anxiogène. Pour les patients, mais aussi pour les professionnels, des données personnelles exfiltrées par les hackeurs peuvent être divulguées sur le web. Au CHU de Rennes, le groupe de cybercriminels Bianlian a publié sur le dark web des fichiers de données du CHU suite à la cyberattaque de juin 2023. « *Bianlian a commencé à mettre en ligne 300 Go de données… On y retrouve des données sensibles comme des données personnelles, des documents financiers, des données du personnel de santé de l'hôpital* » explique Clément Domingo, hackeur éthique rennais. « *Une trentaine de professionnels du CHU a reçu ce jour un mail suspect, non encore authentifié, menaçant le CHU d'une diffusion sur le dark web, de tout ou partie des données ayant fait l'objet d'une exfiltration illégitime* », *« ils n'ont certainement montré qu'une partie des données qu'ils détiennent. Réussir une cyberattaque contre un hôpital, c'est comme un trophée. C'est une manière d'asseoir leur crédibilité envers d'autres éventuels cybercriminels à qui ils pourraient revendre ces données sensibles* » estime Jean-Nicolas Robin, avocat associé du cabinet Avoxa, docteur en droit de la cybersécurité. Ce préjudice envers les patients ou professionnels pourrait donner lieu à d'éventuelles sanctions juridiques : « *On risque d'avoir un boomerang avec les usagers, un retour de bâton possible de la part des associations d'usagers si on laisse diffuser des informations de patients sur le web. On peut aussi imaginer que si les données sont publiées, des recours vont être faits contre les établissements pour dommage et intérêts, défaut de prudence des établissements, manquement à ses obligations de recommandations de bonnes pratiques… Il peut y avoir des avocats qui se saisissent de l'affaire* » (M-D NAEL, CHBA). En effet, les associations d'usagers pourraient se saisir de ces affaires et des recours collectifs pourraient se créer, mettant les hôpitaux visés dans des situations très compliquées.

L’impact en termes d’image est lui aussi important, les cyberattaques sont aujourd’hui de plus en plus médiatisées, la communication doit être maîtrisée, et différents choix sont possibles. Dans le cas du CHBA, le choix a été fait de très peu communiquer, pour notamment éviter d’augmenter sa vulnérabilité mais aussi au regard des préconisations ministérielles.

Les cyberattaques dont sont la cible les établissements de santé peuvent donc aller jusqu’à non seulement paralyser tout ou partie de leur activité dû à l’augmentation de l’utilisation du numérique et de la technologie au sein des activités de soins, mais aussi être à l’origine de fuites de données sensibles hébergées par les établissements. Selon le CERT santé, en 2022, 588 incidents de cyberattaque ont eu lieu visant des établissements de santé, dont 50% d’origine malveillante. L’ANSSI a publié différents guides et référentiels pour que les établissements de santé s’emparent du sujet et soient davantage sensibilisés. Un plan blanc numérique a été publié en juin 2023 afin de doter les établissements des pratiques et réflexes à adopter en cas de survenue d’un incident cyber (évaluation des impacts, cellule de crise...). Les ministères ont réaffirmé la place de la cyber sécurité dans la nouvelle feuille de route du numérique en santé 2023-2027 sortie en mai 2023, un rappel de la posture de l’Etat a aussi été fait quant au non-paiement des rançons lors d’attaques sur les organismes publics, ainsi que la nécessité de porter plainte systématiquement

2 La préparation au risque cyber apparaît dorénavant inévitable et doit se faire de manière interdisciplinaire et opérationnelle : exemple du CHBA

La préparation au risque cyber passe premièrement par la prévention de ce risque via notamment l'acculturation aux bonnes pratiques du numérique, où le rôle du responsable de la sécurité du système d'information a toute son importance (I). La co-construction de plans de continuité d'activité avec les différents services de l'hôpital et le test de ces plans permet d'anticiper des solutions dégradées afin de maintenir la continuité des soins (II). Cependant, ce travail de préparation doit être pensé et mené territorialement dans la mesure du possible, afin de mutualiser retours d'expériences et moyens (III).

2.1 Améliorer la sécurité des systèmes d'information

2.1.1 L'acculturation aux bonnes pratiques du numérique

Malgré la prise en considération croissante des différents enjeux liés à la cybersécurité, on constate que des réticences restent présentes face à ces protocoles et outils au sein du personnel, en raison notamment d'une trop grande complexification dans leurs tâches quotidiennes. Le RSSI d'un établissement de santé a constamment pour objectif de sensibiliser chaque acteur. De plus il est en perpétuelle négociation pour détenir un budget suffisant.

Le gouvernement a pris des initiatives sur le sujet à la suite de la cyberattaque du CHU de Rouen en 2019 : « *Face aux risques de cyberattaques du système de santé, la cybersécurité à l'échelle de chaque établissement de santé est devenue une priorité nationale* » déclarait en 2019 la ministre de la santé de l'époque, Agnès Buzyn. Un plan national de sensibilisation à destination des soignants avait été lancé, et l'Observatoire permanent de la sécurité des systèmes d'information des établissements de santé (OPSSIES) a été créé en 2021 pour cartographier les pratiques des hôpitaux. Le 18 février 2021, Emmanuel Macron disait : « *Notre stratégie en matière de cybersécurité va accélérer. Car il nous faut aller plus loin, plus vite, être à l'avant-garde. Au total, 1 milliard d'euros seront investis. Il nous faut renforcer les formations et doubler à l'horizon 2025 le nombre d'emplois dans ce secteur stratégique. Les structures de santé seront invitées à consacrer systématiquement 5 à 10 % du budget à la cybersécurité, notamment au maintien en condition de sécurité des SI dans la durée* ». En ce sens le ministère de la santé a donc décidé d'engager des moyens afin de mieux préparer les établissements aux situations de crise et de renforcer la sécurité informatique, sous forme de ce que l'on appelle la

« cyberhygiène » : donner conscience des enjeux de sécurité des systèmes dont l'utilisateur se sert quotidiennement. La sécurité relève d'une responsabilité individuelle et collective.

4 axes développent la cyberhygiène et la sécurité des SI :

- La formation (sessions de travail en petits groupes, format hybride, profils différents, logique participative)
- La promotion d'une culture partagée et contextualisée de la sécurité (utilisation de scénarios pratiques, simulations d'attaque..)
- Les mesures de sécurisation
- La protection des actifs numériques par l'exclusion par défaut de tous les accès à l'instruction rationnalisée des besoins d'accès internes et externes : risque de désorganisation important

D'après le ministère de la santé[14], il appartient à chaque structure de santé de mettre en place un dispositif permanant de sensibilisation : des formations internes auprès du personnel, ciblées sur les risques cyber ainsi que des campagnes régulières de sensibilisation. Les établissements peuvent s'appuyer sur les supports nationaux et territoriaux (ARS, CERT Santé, ANSSI, CNIL, MSS, cybermalveillance…).

Le personnel des établissements de santé doit avoir conscience des menaces qui visent les SI et le parc numérique hospitalier. Définir des actions de sensibilisation à la sécurité des SI dans le plan de formation annuel du personnel de l'hôpital et réaliser des exercices théoriques ainsi qu'en conditions réelles est nécessaire.

Intégrer cette problématique dans le plan d'accueil des nouveaux arrivants en insistant sur une sensibilisation forte permet d'initier l'acculturation dès l'arrivée du personnel. La DGOS préconise d'ailleurs de formaliser un document de validation afin de s'assurer que l'ensemble des mesures de sécurité préconisées par l'établissement soient bien comprises par les nouveaux arrivants. Elle préconise de même un affichage permanent des principales recommandations dans les services pour garantir une application des règles de cyber hygiène. L'objectif de ce travail de sensibilisation est que les utilisateurs puissent :

- Prendre conscience des impacts qui découlent d'une attaque cyber par rançongiciel
- Identifier les activités qu'ils doivent maintenir et comment ils peuvent le faire en l'absence des outils informatique à l'échelle de l'établissement : les premières heures, les premiers jours, les premières semaines voire les premiers mois

Concernant le CHBA, le parcours cyber France Relance a montré que le niveau de maturité Cyber du CHBA était très mauvais. Afin de relancer l'économie affectée par la crise

[14] cybersecurite_referentiel_des_mesures_prioritaires.pdf (sante.gouv.fr)

sanitaire liée à la pandémie de Covid-19, le gouvernement a lancé en septembre 2020 le plan « France Relance », comportant notamment un volet cybersécurité doté d'un fonds de 136 millions d'euros. L'objectif de ce volet, piloté par l'ANSSI, est le renforcement de la sécurité des administrations, collectivités et établissements de santé, organismes publics tout en dynamisant l'écosystème industriel français[15]. Il est fondé sur l'implication et le volontariat de ses bénéficiaires et donne accès à un accompagnement adapté au niveau de maturité et aux enjeux de chaque établissement de santé[16]. Le parcours France Relance dans lequel s'est engagé le CHBA lui a notamment permis de faire l'évaluation selon l'ISO 27001 et de partager le résultat à l'échelle de l'établissement (en mai 2023).

L'attaque étant arrivée par la suite en décembre dernier, cela a permis d'une certaine manière une prise de conscience collective. En effet, même une sensibilisation et une préparation accrue ne peuvent permettre une prise de conscience totale sur l'enjeu et les impacts propres à chaque établissement : « *Je pense que malgré les Retex, il est difficile de prendre conscience de l'impact d'une cyberattaque sans l'avoir vécue* », « *il y a toutes les semaines de nouvelles vulnérabilités : attaque par phishing, vulnérabilités sur les firewall, sur les composants Microsoft... Il faut donc sans cesse : veiller, appliquer les correctifs, …* » (C. ALANIC, CHBA). Le travail de sensibilisation, d'acculturation, de préparation aux cyber risques est donc un travail continu. Des actions de sensibilisations sont réalisées au CHBA comme par exemple les campagnes de pishing (cela permet d'évaluer le taux de sensibilisation des professionnels à une forme d'entrée de ce risque), comme celle qui a été réalisée en mai 2023 en sortie de confinement. Le résultat a été le suivant : 10% des utilisateurs du CHBA ont cliqué sur le lien « malveillant ». Ceci prouve que malgré la posture de cybervigilance qui a précédé la campagne, le vécu de la cyberattaque et tout le travail qui été fait, les utilisateurs ne sont toujours pas complètement sensibilisés. « *Des actions étaient réalisées, sont réalisées, et sont encore à ce jour insuffisantes* » (C. ALANIC, CHBA). Pour certains cadres pourtant, la cyberattaque vécue par le CHBA a permis aux agents d'améliorer de manière conséquente leur niveau de culture cyber : « *Les agents apparaissent au clair avec les bonnes pratiques, la cyber attaque vécue a sensibilisé les professionnels, cela a été une opportunité en ce sens* ». (M. MOREL CHBA)

La diffusion et la communication des bonnes pratiques du numérique envers les professionnels est une étape indispensable et peu coûteuse permettant de réduire de manière importante le risque d'intrusion dans les systèmes d'information[17] :

[15] France Relance | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
[16] anssi-france_relance-cybersecurite_proteger_les_etablissements_de_sante.pdf
[17] Les 10 règles de base pour la sécurité numérique - Assistance aux victimes de cybermalveillance

- Adopter une politique de mot de passe rigoureuse : élément souvent négligé et pourtant simple à mettre en œuvre (avoir un mot de passe différent pour chaque accès, utiliser des mots de passe longs et complexes en termes de nombre de caractères, d'alternance minuscules/majuscules/chiffres/caractères spéciaux, changer régulièrement ses mots de passe, ne jamais communiquer son mot de passe à un tiers, choisir des mots de passe robustes et totalement aléatoires)
- Sauvegarder ses données régulièrement
- Etre vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques
- Ne pas communiquer d'information personnelle ou professionnelle par messagerie ou par téléphone
- Se protéger des virus et autres logiciels malveillants (usage exclusif à chaque clé USB pour éviter les contaminations…)
- Ne pas se connecter à un autre réseau que celui de l'hôpital (pas de Wi-fi public ou de partages de connexion)
- Bien séparer ses usages professionnels et personnels
- Ne pas naviguer sur des sites douteux et être vigilant quant au téléchargement de pièces jointes

Les règles de bonnes pratiques sont multiples et l'établissement a un vrai rôle dans la promotion et diffusion de ces dernières.
La sécurisation de la pratique du télétravail est aussi à prendre en compte. Différentes possibilités peuvent être mises en place. En ce qui concerne le CHBA, à la suite de l'attaque le télétravail a dû être suspendu pendant plusieurs mois à cause du confinement. A sa remise en place des changements dans la pratique ont été actés :

- Tous les télétravailleurs ont été dotés d'un ordinateur professionnel afin que le télétravail ne soit pas effectué via des outils personnels
- Une double authentification a été créée grâce à l'utilisation d'un token générant des codes aléatoires et renouvelés à chaque connexion, chaque télétravailleur en ayant un à sa disposition
- Un rappel des règles de bonne pratique du télétravailleur a été fait

« *La construction d'un plan de sensibilisation des professionnels au risque de cyber attaque est important, cela permet la diffusion des bonnes pratiques. Il faut cependant refaire régulièrement des sensibilisations des professionnels. Au CHBA, le plan de formation 2024 devrait contenir des formations obligatoires, comme la sécurité incendie. L'avantage que l'on a est que l'informatique est tellement présent dans nos vies privées*

que cela peut être intéressant pour les professionnels de se former pour maîtriser des pratiques qui leur seront utiles au travail ainsi que dans leur vie personnelle » (M-D NAEL, CHBA). Ces outils sont loin d'être exhaustifs et ne permettent pas d'être sécurisés à 100%. Il faut garder à l'esprit que le travail autour de la sensibilisation des professionnels aux pratiques de cybervigilance doit être réalisé de manière continue et faire partie d'un plan de sensibilisation et de formaiton plus large.

2.1.2 Le rôle du Responsable Sécurité du Système d'Information (RSSI)

Depuis 2012, chaque établissement doit avoir un RSSI nommé. « *Jusqu'à 2019, le rôle du RSSI était plutôt tourné autour de la formalisation, de la documentation, des audits sur la base de questionnaires etc, mais avec peu d'outillage. Depuis les attaques et le renforcement des menaces sur les établissements de santé, le métier a changé* » (C. ALANIC, CHBA)

Le DG de l'établissement désigne ce RSSI afin qu'il mette en place des mesures pour limiter le risque de survenue d'un incident numérique et notamment un incident de cyberattaque : il s'agit du pré-requis P3.1 du programme Hôpital numérique[18] ainsi que de la mesure prioritaire n°6 issue de la dimension Sécurité du référentiel MATURIN'H[19]. Ce référentiel concerne le niveau de maturité numérique des établissements de santé, il s'inscrit dans le cadre de la feuille de route du numérique en santé et fait partie du dispositif de certification des SI des établissements de santé.

Le RSSI est l'interlocuteur privilégié pour la direction et l'ensemble du personnel sur le sujet de la sécurité des systèmes d'information ainsi que la cybersécurité. Il promeut et accompagne les bonnes pratiques de sécurisation et usages, quotidiennement au sein des services de soins, fonction réalisée au niveau GHT. Il va donc inciter les professionnels de l'hôpital à tenir compte des différentes mesures de prévention permettant de limiter au maximum les risques d'intrusion au sein du SI. Il peut à cette fin, mener différents types d'actions : formations, simulations, sensibilisation, information.

C'est donc le RSSI qui est identifié comme l'interlocuteur clé sur la mission de sensibilisation de l'ensemble des acteurs de l'établissement de santé au sujet de la cybervigilance, bonnes pratiques du numériques, prévention des risques numériques. Il définit aussi les actions de sécurisation et en contrôle l'application grâce à ses audits de sécurité et autres diagnostics.

[18] HN_-_Boite_a_outils_pre-requis_-_Fiches_pratiques_-_Octobre_2012.pdf (sante.gouv.fr)
[19] Référentiel MaturiN-H - Ministère de la Santé et de la Prévention (sante.gouv.fr)

Un compte rendu à minima semestriel est aussi effectué par le RSSI auprès de la gouvernance de l'établissement, concernant les avancées dans la mise en conformité du SI, et l'évolution des risques numériques.

Le RSSI travaille avec presque tous les métiers de l'hôpital : direction, services administratifs, services techniques, logistiques, biomédical, médecins, cadres, soignants… La collaboration avec le biomédical est d'ailleurs de plus en plus importante dû à l'augmentation du nombre de dispositifs médicaux connectés au SIH. Le RSSI travaille aussi avec de nombreux acteurs extérieurs à l'hôpital (prestataires, éditeurs, intégrateurs), mais aussi ses collègues RSSI sur le territoire. Le métier de RSSI sera amené à évoluer significativement et de façon continue au rythme des avancées technologiques, réglementaires et des problématiques des établissements.

D'après C. ALANIC, RSSI au CHBA[20], le rôle d'un RSSI est tout d'abord d'éviter que l'établissement soit face à une problématique d'incident cyber et donc d'assurer un niveau de sécurité adéquat pour l'ensemble des établissements du groupement. Les objectifs de sécurité pour atteindre ce niveau sont définis dans la politique de sécurité du groupement, déclinée ensuite en politique de sécurité propre à chaque établissement. Ils portent aussi bien sur la formalisation de chartes (utilisateurs, fournisseurs…) que sur la mise en œuvre d'outils pour protéger le SI et analyser les évènements, que sur la sensibilisation des professionnels et le management de la sécurité. Ils alimentent le plan d'action sécurité.
Des mesures de sécurité doivent être appliquées aux applications et systèmes tant informatiques, biomédicaux que techniques. Elles doivent être définies de manière pertinente en cohérence avec le niveau de sécurité attendu sans bloquer pour autant le déploiement de l'application ou du système, et l'activité des professionnels de santé. Le RSSI est tenu de contrôler leur mise en place et leur respect. Cette démarche doit être intégrée dans les projets. Enfin, l'utilisateur est un maillon important dans la sécurité de l'établissement. Il est le vecteur principal utilisé par les attaquants. Par conséquent, il est important de veiller à la sensibilisation des professionnels pour ancrer les bonnes pratiques mais également les préparer à une éventuelle crise cyber impactant potentiellement l'ensemble du système d'information. Les actions de sensibilisation doivent être permanentes et sous plusieurs formes.
Le niveau de sécurité de certaines applications et du système d'information ainsi que les impacts des actions de sécurisation doivent être évaluées via différents audits : un audit de conformité aux normes en vigueur, audits techniques internes et externes pour détecter les vulnérabilités.

[20] Magazine de la direction commune : B.A.-BA (Brèves et Actualités de Brocéliande Atlantique) n°10

Ces évaluations complètent le plan d'action sécurité du groupement. Certains résultats d'audits imposés sont remontés à l'échelle nationale qui porte une attention particulière à la sécurité du système d'information des établissements de santé.
Dans un contexte de forte menace, le RSSI relaye aux équipes techniques de la DSIT les alertes nationales portant notamment sur des failles de sécurité des composants du système d'information, voire les possibles attaques connues. Il assure la traçabilité et le suivi de ces évènements. Par ailleurs, il traite, avec le concours de la DSIT, les incidents de sécurité qui se produisent en lien avec les instances nationales telle que Cyberveille ou encore l'ANSSI.
Le RSSI assure un reporting de ces actions aux instances de pilotage de la sécurité.

Les RSSI représentent donc un maillon essentiel dans la prévention et la gestion des risques cyber pour les établissements de santé. Cependant, la problématique de la ressource en RSSI se pose : « *Il y a une pénurie de bras plus que de compétences* » alerte André Zaphiratos, « *la rémunération pose problème, même quand on travaille pour le bien commun ». « A l'hôpital, quand un RSSI demande un audit des systèmes à 15 000 euros, parfois il y en a pour 4 mois. Certains jettent l'éponge* » regrette Vincent Trély. Le secteur privé apparaît bien plus attractif d'une part en termes de rémunération mais aussi en termes de réactivité afin de mettre les moyens pour faire avancer les projets.

Au CHBA, la préparation au risque cyber côté « sécurité des systèmes d'information » est toujours en cours. Elle consiste notamment à réaliser une cartographie des applications, des systèmes, des prestataires et des interconnexions.
Lors de la cyberattaque de décembre 2022, le CHBA aurait dû mieux communiquer auprès de ses partenaires : l'EFS, Océlabab, le SIB, .. sur le fait qu'ils étaient en cybervigilance afin que les partenaires soient eux aussi en vigilance. Il n'y avait pas de liste pré-constituée avec les interlocuteurs qu'il fallait informer. De plus, l'identification des applications hébergées à mettre en liste blanche aurait permis un gain de temps.
Cette démarche est faite au niveau de la direction commune. Les applications critiques sont identifiées. Il reste à travailler sur les plans de continuité informatique (PCI) de ces applications.
Une analyse de risques doit être conduite en prenant en compte le risque cyber mais aussi les autres risques pouvant impacter le fonctionnement notamment coupure des services essentiels : électricité, accès opérateurs. Cela a été fléché au Plan d'Actions Sécurité SSI sous réserve d'accompagnement interne (qualité) et externe.

Des actions de sensibilisation doivent être conduites, elles sont aujourd'hui engagées au CHBA. Elles doivent cependant être conduites au niveau groupement du fait de l'interconnexion des sites en privilégiant toutefois les applications critiques.

2.2 Formaliser des plans de continuité d'activité

2.2.1 Construire des plans de continuité d'activité opérationnels

Les établissements de santé vont donc devoir travailler sur un plan de continuité d'activité en cas de cyberattaque, afin de se préparer et anticiper des solutions pour permettre la continuité de l'activité de l'établissement. La priorité est placée tout particulièrement autour des activités les plus critiques, préalablement identifiées, dans un environnement dégradé. Le PCA a donc pour objectif d'identifier des scenarios par risque ou type de risque (incendie, coupure d'électricité, cyberattaque..) et y oppose des réponses préalablement travaillées et donc opérationnelles et connues en prenant en compte les différents impacts ainsi que leurs conséquences sur l'activité. Ce plan de réponse doit être validé par la Direction, laquelle est impliquée à toutes les étapes de la gestion de crise. Les éléments suivant doivent être travaillés au sein des services, avec un scénario à identifier (exemple : « *absence totale d'accès au système d'information informatisé et téléphonique* ») et un objectif (exemple : « *définir le niveau de production de soins possible en sécurité pour les patients et les professionnels au moment de l'arrêt du système (T0) et jusqu'à 24h* ») :

- Inventaire des actifs à protéger (systèmes, réseaux, informations, produits..)
- Identification des types de données nécessaires au maintien de la prise en charge patient (données inter établissements, inter services, données patients…)
- Identification des liaisons téléphoniques indispensables
- Contrats conclus avec prestataires externes
- Attribution et recensement des responsabilités de chaque acteur

Avant l'attaque cyber du CHBA, le travail des plans de continuité d'activité n'avait pas encore été engagé. « *L'établissement dans sa globalité, les acteurs n'étaient pas préparés, n'avaient pas réfléchi à un plan de continuité. Nous étions finalement presque au niveau zéro quand on se place à l'échelle de l'établissement* » (V. JOUVET, CHBA) ; « *L'établissement n'était pas prêt à vivre une cyberattaque, tant côté informatique avec ses PCI (Plan de Continuité Informatique) que coté métiers avec les PCA qui n'étaient pas suffisamment pragmatiques et surtout non testés* » (O. PLASSAIS, CHBA) ; « *L'établissement n'était clairement pas prêt. Avec la DDS, un travail était initié sur la*

création d'un dossier patient papier en cas de black out mais celui-ci n'était pas prêt ni validé. Ce n'était clairement pas une priorité » (S. TECHER, CHBA) ; « *On savait qu'on devait le faire, c'était identifié dans le programme de travail mais on n'était pas préparés à vivre une cyberattaque. Niveau très faible, pour ne pas dire inexistant* » (M-D NAEL, CHBA).

Avec un niveau de préparation très limitée, le CHBA s'est mobilisé pour produire en moins d'un mois des PCA de qualité. Même si le travail n'est à ce jour pas encore terminé, le niveau d'avancement n'a jamais été aussi élevé et en un temps record, grâce à la forte mobilisation des professionnels : « *La mobilisation au CHBA a été exceptionnelle notamment pendant les fêtes de Noël et cela grâce à l'implication du DG »* (O. PLASSAIS, CHBA). « *La mobilisation des professionnels a été essentiellement à des niveaux de responsabilité : équipe de direction, chefs de pôles, cadres coordonnateurs de pôles, chefs de services, cadres de santé, adjoints de direction. Il leur a été demandé de formaliser leur PCA. 3 directions ont été plus particulièrement mobilisées : DSIT, DS, DPQGDR* » (M-D NAEL, CHBA). Les différents entretiens menés se sont tous accordés à dire que dans l'urgence, alors que l'attaque a eu lieu en pleine semaine de certification, la mobilisation a été au rendez-vous, chaque acteur ayant à cœur de jouer son rôle. La mobilisation a donc été forte, avec une déclinaison opérationnelle d'actions qui ont nécessité une réactivité importante ainsi qu'une disponibilité sans faille de la part des équipes. Dans ces moments, la bonne connaissance des acteurs à mobiliser est essentielle et permet de ne pas perdre de temps précieux. Il est important que chaque acteur dans son domaine de compétence soit entendu, et qu'une terminologie commune soit partagée, notamment entre le soin et l'informatique afin de prendre des décisions communes en toute connaissance de cause.

Le PCA est indispensable pour un établissement afin d'être correctement préparé en amont de la crise, il est comme une « boîte à outils », un « guide » qui va aider l'établissement à faire face à la crise avec le plus d'éléments d'anticipation possible grâce d'une part à l'identification la plus exhaustive possible des différents impacts de l'incident en question, et d'autre part aux différentes solutions dégradées préalablement proposées, travaillées et même testées. Il découle des PCA des process qui permettent de maintenir l'activité en limitant le plus possible les impacts et le délai de réponse.
Ainsi, le PCA repose sur l'identification des risques, l'analyse des vulnérabilités de l'établissement, permettant de définir les services les plus sensibles, les plus critiques en matière de continuité des soins, puis les étapes permettant de maintenir cette continuité.
Il paraît essentiel que le PCA intègre la définition du rôle de chacun et éventuellement différents scénarios possibles. De plus, il doit être mis à jour régulièrement et doit faire

partie des documents à modifier lorsque l'organisation d'un service ou une de ses procédures change et a un impact sur le contenu du PCA.

Concernant l'expérience du CHBA, étant dans un contexte d'urgence liée à l'alerte, de période de certification et approchant des périodes de fin d'année, il n'a assurément pas été possible de mener ce travail pour l'ensemble des établissements de la direction commune en même temps. Le parti pris a été de sécuriser le CHBA car c'est l'établissement qui était attaqué, puis tester et roder les plans de continuité pour ensuite les diffuser progressivement au centre hospitalier de Ploërmel et aux autres établissements de la direction commune. « *Il fallait que l'on puisse assurer fonctionnement des 48 – 72 premières heures »* (M-D NAEL, CHBA). La préparation a consisté en deux grandes parties :

- Une première partie « technique » d'identification des mesures de sécurisation des infrastructures numériques pour assurer la continuité des prises en charge, suivi du volet « plan de remédiation »
- Une seconde partie plus « organisationnelle » consistant à travailler sur les PCA pour réfléchir à comment faire face à une cyberattaque et donc une indisponibilité totale du système d'information. L'hypothèse du pire scénario a été choisie, c'est-à-dire d'un black-out total de l'informatique.

L'idée était qu'il fallait construire le plan de continuité de l'établissement, fondé sur le plan de continuité des différentes unités et services de l'hôpital (techniques, médicotechniques, de soins, administratifs..). L'outil de PCA a été construit en partant d'une feuille blanche, et tous les secteurs ont été sollicités pour compléter cet outil dans des délais particulièrement courts (une semaine). Une fois les PCA des unités remontés au niveau de la DPQGDR, une relecture service par service a été effectuée ainsi qu'une relecture transversale. C'est à ce moment que le laboratoire a été identifié comme le cœur du réacteur de l'hôpital, aux côtés de l'imagerie notamment car ils conditionnent la continuité d'activité des autres services. Une lecture croisée a ensuite été faite afin de faire apparaître ce sur quoi il fallait travailler en fonctions des priorités, ce qui a amené à définir un plan d'action des mesures palliatives pour répondre dans les 48-72 premières heures :

- Caisses cyber créées et mises à disposition dans les unités de soins avec une téléphonie de secours ainsi qu'un ou plusieurs PC vierges avec clé 4G permettant en situation de crise cyber d'accéder aux dossiers des patients présents au moment de l'attaque
- Un annuaire plan blanc a aussi été créé
- Procédures de rappel

Des temps de présentation de ces outils ont été faits aux cadres coordonnateurs de pôles ainsi qu'aux cadres de santé afin que les services aient connaissance des outils, de leur contenu et leur fonctionnement…
Au fur et à mesure des mois et notamment lorsque l'établissement a été « déconfiné », le soufflet est retombé. En effet, le confinement internet a représenté une contrainte non des moindres chez les professionnels et le souhait de mettre fin à ce confinement a continué à motiver les équipes sur le travail du risque cyber. Ce travail de préparation continue toujours, seulement avec moins d'urgence et de pression maintenant que l'évènement est maîtrisé et sous contrôle.

Au-delà des PCA des services, le travail complémentaire autour du SI de l'établissement et de sa sécurisation a été engagé avec de nombreux objectifs, mais qui nécessitent du temps : « *Sur le plan des PCA, ils sont au moins en partie opérationnels, sur le plan informatique, il reste encore beaucoup d'investissement à réaliser sur les 2 prochaines années. Il est impossible de refondre un SI en quelques mois, le travail sera de longue haleine … mais le niveau de sécurité actuellement est jugé satisfaisant par Orange Cyber Défense »* (O. PLASSAIS, CHBA)

Cette crise cyber, au-delà des dysfonctionnements qu'elle a généré et de la pression qu'elle a fait subir, est considérée par l'établissement comme une opportunité qui a accéléré de manière sans précédente un travail de préparation au risque, et a permis à l'établissement de prendre conscience des impacts d'une cyberattaque : *« Honnêtement, je pense que collectivement nous avons bien géré cette crise mais avons aussi eu beaucoup de chance »* (M-D NAEL, CHBA) ; « *cela a été une vraie opportunité d'être alerté très en amont, et de n'être pas d'emblée plongés dans le noir. Côté positif : l'alerte donnée a permis d'anticiper les choses, c'est une vraie chance d'avoir été prévenu tôt* » (P. COUTURIER, CHBA) ; « *La crise a été une opportunité, car l'établissement a compris qu'il fallait investir sur les systèmes d'information et leur sécurité, et aussi car les services se sont engagés dans leur PCA grâce à cette alerte* » (C. ALANIC, CHBA).

2.2.2 Tester ces plans de continuité d'activité grâce à la réalisation d'exercices

En juin 2023, 6 mois après la cyberattaque, le CHBA a organisé un exercice avec une société spécialisée dans la réalisation d'exercices cyber. L'exercice a permis de déclencher les procédures sur un périmètre réduit (2 services participants : le standard et la neurologie).

L'organisation d'exercices, de simulations, de formations permet non seulement la sensibilisation des équipes mais aussi leur entrainement afin d'être le plus opérationnel possible le jour J.

Les objectifs de l'exercice sont les suivants :

- Identifier les forces et les axes d'amélioration dans la gestion d'une crise type cyber et repérer les axes de travail par rapport à la directive de gestion de crise cyber
- Tester et renforcer la capacité d'organisation des acteurs dans le cadre d'une crise affectant les SI
- Renforcer le vécu et la coordination entre des acteurs de différents secteurs dans un contexte de crise

L'identification des tests et exercices comme élément à part entière dans la préparation d'un établissement de santé à une cyberattaque est partagée par toutes les personnes interrogées *: « Il faut organiser des exercices de gestion de crise cyber en se passant de l'informatique » (O. PLASSAIS, CHBA) ; « Beaucoup d'agents sont très intéressés pour participer à des tests ou exercices, certains étaient même presque déçus de ne pas avoir été là le jour du dernier exercice* », « *comme ils ont une forme d'appréhension, les tests les rassurent beaucoup* », « *avoir un retour sur ces exercices est aussi très important afin que tout le monde puisse bénéficier de l'apprentissage tiré notamment* » (M. MOREL, CHBA).

Lorsqu'un exercice est programmé, il faut délimiter le cadre de cet exercice, les personnes participant à l'exercice, les personnes observatrices de l'exercice ainsi que ses objectifs. En effet, on ne peut pas tout évaluer en même temps, il faut cibler quel est le but de l'exercice en question (test d'une procédure, communication, fonctionnement d'une cellule de crise, opérationnalité d'outils…). Les exercices réguliers permettent aussi à l'établissement et à ses services de mettre à jour leurs procédures dégradées.

Les exercices ont cependant des biais dont il faut avoir connaissance en amont : « *L'exercice que nous avons fait en juin était biaisé. Cela permet en effet d'aller tester ce que nous avons mis en place et nous assurer que c'est opérationnel. Mais c'est difficile car l'exercice est littéralement condensé en un temps record. Dans la vraie vie, c'est beaucoup plus long.* » (V. JOUVET, CHBA). Effectivement, la cinétique des exercices peut être beaucoup plus courte qu'en situation réelle, induisant un biais non négligeable dans la manière de répondre à la crise.

Au-delà de l'aspect technique des procédures à tester, l'aspect humain est également déterminant lors d'une gestion de crise. En effet, la gestion de crise n'est pas une somme de procédures à suivre mécaniquement mais est avant tout une gestion d'évènements réalisée par des femmes et des hommes dont il faut comprendre les ressorts psychologiques et guider le fonctionnement. L'exercice, qui lui aussi doit être préparé apparaît comme un élément clé du succès permettant d'améliorer la performance de la coordination entre les différents acteurs.

Tout exercice doit bien évidemment, comme tout incident ou crise réellement subi, faire l'objet d'un retour d'expérience afin d'en tirer les bénéfices souhaités, d'étudier les éléments positifs et moins positifs, et d'en dégager des actions à mettre en place.

2.3 Se préparer de manière territoriale en mutualisant expériences et réponses communes

2.3.1 L'importance du partage des retours d'expérience

Le CHBA n'a à ce jour toujours pas réalisé de réel retour d'expérience de la crise cyber qu'il a vécue en décembre dernier. La nécessité de réaliser ce RETEX a été identifiée mais l'occasion n'a pas encore été provoquée, le travail de réalisation d'un RETEX étant long et fastidieux, le calendrier de chacun n'ayant jusqu'ici pas laissé place à ce dernier.
Cependant, nous pouvons prendre l'exemple du RETEX qui a été réalisé suite à la panne électrique qui avait touché différents services dont des services critiques du CHBA en octobre 2022. Ce dernier a permis de repasser à froid la temporalité de l'évènement et des décisions prises, ainsi que le vécu de chaque acteur, des besoins identifiés et un plan d'action. D'après Crysalide, société choisie par le CHBA pour effectuer son exercice de cyberattaque, le RETEX a un objectif fonctionnel, humain et pédagogique, et permet de :

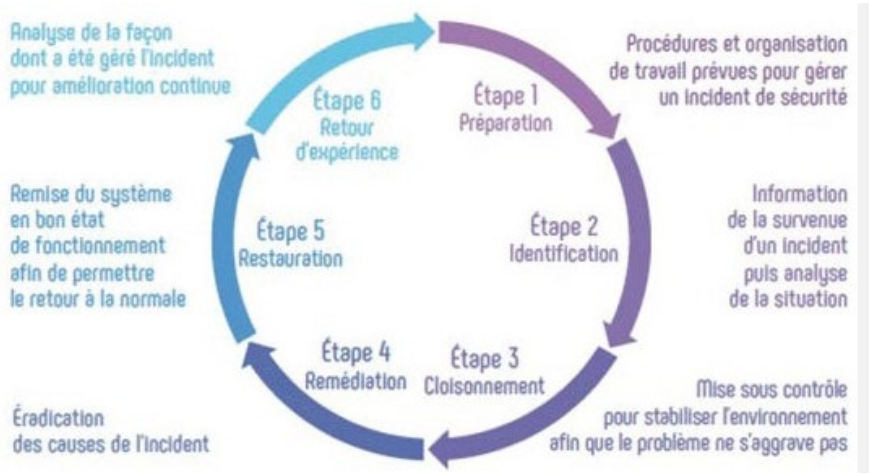
- Partager une vision globale de l'évènement et renforcer les liens entre équipes
- Repérer les points positifs et les capitaliser : identifier les pratiques positives (techniques, compétences humaines ou organisationnelles) et les porter à la connaissance des différents acteurs qui pourraient être confrontés à la gestion d'un évènement semblable dans l'avenir.
- Identifier les points négatifs et proposer les axes d'amélioration : le RETEX n'est pas une sanction, il dégage les points de dysfonctionnements en toute impartialité et met en avant l'amélioration des pratiques qui est attendue.

- Permettre la reconnaissance du travail de chacun et faciliter la résilience : le RETEX est l'occasion de prendre acte de l'investissement de chacun dans la gestion de l'évènement, de valoriser le travail des différents acteurs et leur permettre de rebondir et d'aller de l'avant
- Valoriser l'expérience acquise pour la gestion des évènements futurs : élaboration, mise à jour et diffusion de procédures ou de plans, impulsion de l'évolution de la réglementation
- Démultiplier les enseignements tirés et sensibiliser les acteurs potentiels : le RETEX est porté à la connaissance de tous et pas seulement des acteurs concernés par l'évènement. Il permet d'améliorer les pratiques et les connaissances de manière générale.

Le RETEX a une méthodologie adaptée pour chaque évènement qu'il étudie. Des étapes identifiées doivent être suivies pour sa conception :

- L'identification d'un pilote : le pilote doit être une personne neutre vis-à-vis de l'évènement pour avoir une approche la plus objective possible. Ce dernier est chargé de collecter et analyser les informations, de recueillir les différentes expériences et d'animer la réunion de restitution du RETEX. Le pilote peut être entouré d'une équipe afin de l'accompagner dans cette démarche.
- La définition des objectifs stratégiques et opérationnels
- La définition d'un périmètre (en termes d'acteurs, mais aussi un périmètre temporel et géographique)
- La détermination d'un calendrier de réalisation : il est souvent conseillé de réaliser en première intention un RETEX « à chaud » juste à l'issue de la crise. Ce dernier permet de collecter des premières informations, mais aussi d'évacuer des ressentis, dans la neutralité et dans l'unique objectif d'amélioration continue. Il faut ensuite se laisser le temps de la collecte d'informations, de l'analyse et de la prise de recul afin de programmer une date pour le RETEX « à froid » une fois toute la méthodologie menée. Le RETEX « à froid » est beaucoup plus long et complet que le RETEX « à chaud ».
- La collecte des informations et l'analyse des données (entretiens individuels, réunions de partages...)
- La diffusion du RETEX à tous : une diffusion ouverte au plus grand nombre, l'objectif étant de tirer leçon de l'évènement passé et de donner les clés au plus grand nombre pour de potentiels évènements futurs.

- La mise en œuvre des préconisations ainsi que le suivi de cette mise en œuvre : le RETEX a aussi donné lieu à un plan d'action avec un certain nombre de préconisations à mettre en place pour prévenir davantage les risques et être mieux préparé
- La valorisation du RETEX : étape souvent négligée, consistant à partager son RETEX au-delà de son établissement. L'ARS a un rôle dans le partage de ce RETEX et dans son animation.



2.3.2 Organiser une réponse commune et mutualiser les moyens

La menace cybercriminelle concerne tout type d'établissement, quels que soient leur taille, leur positionnement, leur rôle, et les ARS doivent accompagner les établissements de leurs territoires dans cette préparation au risque cyber. Pour contrer cette menace, il faut veiller à intégrer systématiquement les enjeux de cybersécurité dans les différents cahiers des charges, et que l'enjeu de cybersécurité devienne comme l'enjeu de la prévention des risques ou de la qualité des soins un enjeu à part entière de la politique des établissements.

Les moyens doivent être mutualisés entre les établissements et non saupoudrés individuellement. Vincent Trély alerte sur cet écueil : *"Mutualisons la gouvernance, la feuille de route, le RSSI …Le pire serait de dire : on va donner un peu d'argent à tous, parce que tous auraient alors une faible protection, à 50 000 euros chacun, pas très efficace."*
Un réseau de RSSI a déjà été créé afin de favoriser l'entraide dans le cas d'une crise au sein d'un établissement. Dès lors, le réseau peut être mis à disposition de l'équipe de direction de l'établissement attaqué.

« *Je déplore le fait que chaque établissement travaille dans son coin, c'est dommage car tous les établissements n'ont pas les mêmes moyens, en particulier les petits établissements autonomes. Dans notre cas, les plus petits établissements de la direction commune vont pouvoir bénéficier de nos organisations, mais je m'interroge de ce qu'il va en être pour d'autres* » (M-D NAEL, CHBA). Nous sommes en effet encore sur des approches établissement-centrées, sauf qu'il manque un niveau entre le national et le terrain, un niveau intermédiaire, régional qui accompagne les établissements. Il faut identifier les problématiques communes, les moyens à mutualiser, et accompagner les établissements qui n'ont pas les compétences ni les ressources pour se préparer seul à ce risque. Le guide plan blanc numérique national de la DGOS sorti en juillet dernier, bien que donnant de nombreuses pistes pour préparer les établissements de santé aux incidents cyber, prend difficilement en compte le fait que tous les établissements de santé de France ne disposent pas d'un service informatique hyper pointu. De plus, ce travail de préparation devrait pour une partie au moins être mutualisé entre plusieurs établissements en fonction des territoires. Par exemple, le travail autour des plans de continuité d'activité va potentiellement être fait dans certains établissements en partant d'une feuille vierge, au lieu de s'inspirer de ce que les établissements voisins ou établissements comparables de par leur taille et/ou leur activité ont déjà réalisé. « *Il faut que l'on mutualise ces travaux, chaque établissement ne peut pas travailler seul dans son coin, mutualiser permet d'éviter les écueils, nous avons tous beaucoup à y gagner* » (M-D NAEL, CHBA)

Il paraît important de partager le vécu d'une attaque, le résultat des réflexions aux autres établissements. Dans le cas du CHBA, il a notamment été identifié qu'il faut investir dans un certain nombre d'infrastructures de suppléance avec un coût non négligeable. Initier une réflexion avec les établissements voisins pour mutualiser des équipements, des stocks afin de partager les coûts dans une logique de maîtrise des dépenses des deniers publics d'une part, et d'autre part pour en faire bénéficier les petits établissements. Avoir des stocks communs de matériels (sténorettes, GSM de secours…), financés par plusieurs établissements apparaît logique pour répartir le montant de l'investissement.
Pour élargir le propos, une réflexion autour d'un plan cyber régional devrait être initiée. Le rôle de l'ARS dans l'animation de cette réflexion peut être utile et permettre de coordonner la réflexion et construire ce plan régional.

3 L'efficacité de la préparation au risque et de sa réponse passe nécessairement par une acculturation diffuse à la gestion des risques, à la qualité et au management de crise

La Direction de la gestion des risques, souvent associée à la Direction de la qualité occupe une place de plus en plus conséquente à l'hôpital au vu des exigences croissantes en matière de qualité et de sécurité des soins (I). L'acculturation des équipes à la gestion des risques apparaît inévitable pour que les travaux de préparation aux risques puissent être mis en place, mais représente un vrai challenge (II). La préparation aux risques, pour être complète, doit aller jusqu'à travailler le management de crise, anticiper l'organisation de la cellule de crise d'une part, et son plan de communication d'autre part (III).

3.1 La Direction qualité et gestion des risques occupe une place de plus en plus importante à l'hôpital

3.1.1 Une direction nouvelle qui connaît de nombreux défis

La direction qualité et gestion des risques est aujourd'hui au cœur des enjeux de l'hôpital. Les exigences en termes de qualité et de sécurité des soins qui incombent aux établissements de santé illustrent l'importance d'un management fort qui impulse de larges travaux sur ces nombreux sujets.

Le secteur de l'industrie est à l'origine du développement du management de la qualité. Les établissements de santé, producteurs de soins, ont progressivement introduit cette politique avec les notions de référentiel, accréditation, traçabilité, certification. La démarche qualité et gestion des risques a été progressivement mise en place à partir des années 1990 à la suite de scandales sanitaires, et ont été fixées par un premier cadre juridique avec les ordonnances Juppé (24 avril 1996), mettant en place l'évaluation externe obligatoire des établissements de santé. L'Agence Nationale d'Accréditation et d'évaluation de la Santé (ANAES) a donc été créée pour piloter cette démarche d'évaluation externe, remplacée par la suite par la Haute Autorité de Santé (HAS). Cette démarche qualité et gestion des risques a progressivement évolué depuis 1996, marquée par les différentes certifications. Les enjeux de cette démarche sont plusieurs :

- L'amélioration continue des pratiques de la qualité et de la sécurité des soins au bénéfice des usagers
- La maîtrise des risques en repensant les organisations et en renforçant la culture qualité-sécurité

- Un enjeu financier de maîtrise des coûts
- Un enjeu managérial envers les professionnels
- L'enjeu de réponse aux besoins des usagers

La dynamique de la gestion des risques implique donc que chaque acteur de l'hôpital soit engagé. La participation des professionnels à cette démarche est néanmoins parfois vue comme une obligation, notamment en période de certification, vécue comme une charge de travail supplémentaire. Le contexte financier des établissements de santé imposant des réorganisations régulières liées au manque de ressources monopolise les professionnels et peut faire passer la démarche qualité et gestion des risques au second plan.

A l'hôpital, le management de la qualité et de la gestion des risques est souvent confié à un directeur d'hôpital adjoint. Les principales missions de la Direction qualité et gestion des risques s'articulent autour des axes suivants :

- Développer la culture de l'évaluation et de l'audit centrés sur le patient
- Porter la démarche de certification de la HAS
- Accompagner les équipes dans leurs démarches d'amélioration continue de la qualité et gestion des risques
- Mettre en œuvre un management de la qualité et gestion des risques

L'expérience du stage long à l'hôpital permet entre autres d'appréhender les différentes directions non seulement d'un point de vue « missions et objectifs », mais aussi d'un point de vue « personnalité » et exigences managériales et humaines pour atteindre les objectifs définis pour chaque direction. Cela permet de se projeter ou pas dans telle ou telle direction, premièrement pour le poste en sortie d'école, mais aussi pour la suite, en fonction d'appétences techniques, de personnalité, de quotidien de travail que représente chaque direction. Même si cela varie aussi en fonction de l'établissement, on peut tout de même étudier différents profils. En ce sens, le Directeur en charge de la gestion des risques doit avoir une personnalité forte pour faire face aux réticences qui font partie inhérente du quotidien de cette direction, ainsi que des capacités relationnelles importantes afin d'être un ambassadeur de la gestion des risques et de réussir à fédérer les différents acteurs autour et de les sensibiliser, pour qu'ils s'investissent dans ces projets.

3.1.2 Une direction qui nécessite un soutien capital de la part de la Direction Générale et une collaboration étroite avec la Direction des soins pour mener à bien ses politiques

Le soutien de la Direction Générale est primordial afin de mener une politique de gestion des risques au sein d'un établissement de santé. Le DG et le PCME définissent cette politique de qualité et gestion des risques et impulsent une dynamique institutionnelle. L'engagement de la direction doit être formalisé dans le projet d'établissement, avec son positionnement au sein de l'institution, et les moyens qui sont allouées à cette démarche qualité gestion des risques, ces éléments sont déterminants pour cadrer institutionnellement le management qualité gestion des risques.

Si l'on prend l'exemple du CHBA, le travail réalisé sur les plans de continuité en cas de cyber attaque n'aurait pas pu être fait sans le soutien de la Direction Générale. Le mot d'ordre était clair et la demande est partie de la Direction Générale, afin d'incarner l'importance et l'urgence de ce travail.

Au-delà du soutien de la DG, la Direction de la gestion des risques nécessite d'être soutenue par l'ensemble de l'équipe de direction. Prenons l'exemple des directeurs de pôle, qui ont aussi pour rôle de relayer de la part de la direction les demandes de travaux sur tel ou tel projet au sein des services de leur pôle. En communiquant sur les projets et sur l'importance de ces derniers, sur les échéances à respecter, ils appuient la démarche et cela conditionne la bonne appropriation par les équipes.

La collaboration avec la Direction des soins est elle aussi au cœur de la performance de la démarche qualité et gestion des risques. Le projet de soins doit être cohérent et en accord avec le projet qualité et gestion des risques. La commission de soins est d'ailleurs consultée sur cette politique et la Direction des soins contribue au pilotage de sa mise en œuvre en lien avec l'encadrement et la communauté médicale.
Les interactions entre la Direction qualité gestion des risques et la Direction des soins sont un vrai enjeu et elles doivent partager une vision commune et complémentaire à ce sujet. Si ce n'est pas le cas, cela peut représenter un réel frein pour faire avancer les projets.

En effet, pour que les travaux de préparation aux différents risques auxquels est confronté l'hôpital avancent , c'est l'ensemble de la direction qui doit apporter son soutien, d'autant plus que les projets et sollicitations sont multiples à l'hôpital et s'accumulent

tellement que préparer son service face au risque de cyberattaque ou encore de rupture d'alimentation électrique peut très vite passer en-dessous de la pile des priorités.

3.2 L'acculturation des équipes à la gestion des risques : un vrai challenge à l'hôpital

3.2.1 Sensibiliser les équipes dans un contexte de sursollicitation

Les établissements de santé rencontrent bien souvent des contraintes liées à la culture du risque cyber chez le personnel soignant. L'acculturation à n'importe quelle thématique est quelque chose qui se construit sur le temps long. Une des problématiques qui se pose dans l'acculturation des équipes à la gestion des risques est cette différence de temporalité entre ce qu'ils vivent : le court terme, l'urgence, la priorisation permanente de leurs tâches/missions et entre ce qui est nécessaire pour s'acculturer aux thématiques de la gestion des risques : travaux interdisciplinaires, demandant du temps régulier, n'étant pas considérés comme une priorité pour beaucoup d'entre eux.

Le management de la qualité et de la gestion des risques suscite souvent des craintes et des résistances de la part des professionnels. Différents types de freins peuvent être identifiés :

- Un manque de formation
- Une communication inadaptée
- Un manque de collaboration entre la Direction qualité gestion des risques et la Direction des soins
- Un programme trop théorique en décalage avec le niveau de préparation du terrain

Ces freins et craintes doivent être pris en considération pour adapter la démarche qualité et gestion des risques, surmonter ces résistances, et créer des conditions de succès. Au sein des établissements, un panel varié de professionnels différents existe, avec de nombreuses visions de la gestion des risques et des objectifs différents en fonction des perceptions. Les méthodes de travail doivent être claires et s'adapter à l'organisation afin d'éviter les difficultés d'appropriation et les confusions. L'objectif de la démarche qualité qui est d'optimiser les organisations au service des usagers et la qualité et la sécurité des soins est fondamentalement commun avec celui des professionnels, et cela doit être compris et entendu des deux côtés afin de favoriser la poursuite de cet objectif.

C'est souvent l'encadrement qui est le premier sollicité sur ce type de travaux et les sujets sont nombreux. Les cadres sont en premier lieu très sollicités sur la gestion du personnel, le management des équipes mais surtout sur des problématiques d'absentéisme récurrentes et permanentes qui viennent littéralement monopoliser leur quotidien. De plus,

ils sont le lien de terrain de la Direction des soins pour mettre en place les différents projets, études, travaux.

Ces sujets ne concernent pourtant pas uniquement l'encadrement, mais bien l'ensemble des équipes, et il est du rôle aussi du chef de service en tant que hiérarchique médical du service de s'investir dans ce travail et de sensibiliser la communauté médicale qui se sent généralement plus ou moins concernée en fonction des sujets. Pour le travail de PCA cyber organisé au CHBA, la demande a été adressée non seulement aux cadres mais aussi aux chefs des différents services de l'hôpital. Les sujets ne peuvent en effet pas être traités de manière complète sans la contribution du personnel médical.

Le constat a été fait pendant cette préparation au risque cyber qu'il y a autant de manières de travailler, de pratiques différentes que de services dans l'hôpital allant pour certains services à l'unique relais du cadre jusqu'à un investissement très important du chef de service et un réel travail en commun. Les nombreux rendez-vous et réunions de préparation des PCA l'ont montré. « *L'appropriation par tous les niveaux de responsabilité du risque et de ses impacts, mettre en œuvre des modes de fonctionnement qui intègrent la gestion de risque, c'est passer par un management par la qualité. Plus on avance plus on est dans un environnement qui justifie d'être dans la gestion des risques* » (M-D NAEL, CHBA). La plus-value n'est pas toujours perçue par les professionnels car pas forcément visible à court terme notamment. « *A Vannes, on a même du mal à mobiliser les gens sur la formation incendie* » (P. COUTURIER, CHBA), le risque incendie paraissant pourtant un risque communément entendu comme important, où les conséquences peuvent être fatales. Organiser les formations incendie pour chaque agent tous les 3 ans comme cela est règlementairement prévu n'est aujourd'hui pas réalisé au CHBA malgré les nombreuses sollicitations pour faire inscrire les agents.

Le management doit donner du sens aux démarches afin notamment de mieux comprendre les attendus. L'implication et la participation active du personnel dans ces démarches est indispensable. La HAS souligne d'ailleurs que le management de la qualité et de la gestion des risques est positionné en tant que processus de pilotage, à un niveau stratégique et opérationnel et implique un réel engagement de la Direction. L'enjeu est d'élaborer une stratégie managériale qui permette une approche participative des professionnels à l'amélioration continue.

3.2.2 Le constat de temps et de compétences dédiés nécessaires à l'accompagnement des services

Le constat qui vient d'être fait autour de la difficulté à solliciter les équipes sur d'énième thématiques qui viennent se rajouter à un quotidien de gestion de l'urgence permanente amène à repenser la manière de mobiliser les équipes à la gestion des risques.

Un accompagnement s'avère nécessaire pour d'une part les guider dans ces travaux et leur faire gagner du temps, mais aussi pour cultiver tous ces travaux et éviter qu'ils finissent par ne plus être à jour ni être à la connaissance des équipes.

Le travail de communication est indispensable pour que ces outils soient utiles et qu'ils évitent d'être des procédures supplémentaires qui ne sont connues que de quelques personnes et ne seront pas utilisées en cas réel.

Comment organiser ce temps dédié ? A qui revient la « tâche » de concevoir des plans de continuité d'activité ? A quel besoin en ETP cela correspond-il ?

Au-delà du facteur établissement-dépendant, la notion de PCA concernant la gestion des risques se rattache à la Direction qualité et gestion des risques qui paraît être légitime à en organiser la conception. Le chef de projet devrait donc être éventuellement rattaché à la Direction qualité et gestion des risques et avoir d'une part une compétence technique d'ingénierie et d'autre part une réelle compétence managériale qui sera l'essentiel de son rôle. Déléguer ce type de projet à un profil ingénieur qualité apparaît adapté. En effet, tout ingénieur est acculturé à la gestion de projet mais il faut en plus que l'ingénieur ait une compétence en gestion des risques.

Ce dernier devra cadrer la stratégie projet, coordonner l'avancée du projet, animer des groupes de travail, mettre en place des outils de suivi, et faire le lien permanent entre les différentes parties prenantes du projet.

La démarche projet sera essentielle pour réussir à obtenir le résultat souhaité. Cette dernière repose sur :

- Un cadrage robuste des projets : la préparation au projet est une étape clé de la réussite d'un projet car elle va préciser les enjeux, objectifs et résultats attendus et valider ces derniers de façon concertée. La mobilisation de l'intelligence collective est primordiale, passant par un travail participatif et transversal qui est cadré et validé en amont.
- Un suivi efficace grâce à un reporting structuré et une coordination d'ensemble. Le reporting doit être régulier, fait par le chef de projet à chaque étape du projet. Cela permet de s'assurer de l'atteinte des résultats au regard des objectifs fixés.

- Une visibilité à ne pas négliger passant par une communication organisée aux différentes étapes du projet. Cette communication peut se faire selon différentes modalités définies par le groupe projet.
- Des outils et un appui méthodologique. L'appui est réalisé en continu par la Direction des projets / qualité gestion des risques.

Le chef de projet va animer et coordonner le projet. Il va le mener grâce à l'appui d'un groupe projet, qui peut lui-même traiter certains travaux avec des groupes de travail ad hoc. Il réunit régulièrement son groupe projet. Il faut donc prendre la gestion des risques comme de la gestion de projet. La personne référente, chef de projet, identifiera des personnes supports pour répondre de manière ponctuelle au chef de projet (permettant d'être en permanence à jour dans le travail de benchmark).

« On voit que la gestion des risques nécessite d'avoir des ressources dédiées, c'est se leurrer de croire que non », « c'est un métier, cela nécessite du temps, beaucoup de structuration, de conception des plans de sécurisation, de suivi des alertes… » (M-D NAEL, CHBA). La définition de temps dédié est aussi essentielle au bon déroulé du projet. Cela fait partie de la méthodologie projet : estimer un temps, le réévaluer à échéance prédéfinie, reconnaître ce temps (30% d'un ETP par exemple pour un chef de projet), mais aussi pour les personnes travaillant régulièrement sur le projet. Cela induit soit un transfert de missions soit une priorisation des projets.

3.3 Savoir manager en temps de crise, un exercice exigeant qui conditionne une bonne gestion de crise

3.3.1 Le bon fonctionnement d'une cellule de crise hospitalière et sa professionnalisation

« *Le problème n'est pas de se préparer pour éviter les surprises, mais se préparer à être surpris* » - Todd LaPorte

Les scenarios et plans suite aux situations sanitaires exceptionnelles ne se déroulent jamais exactement comme prévu, malgré une bonne anticipation et une préparation complète et opérationnelle face aux risques. En effet, la complexité des crises sanitaires suppose une réelle destruction des références utilisées quotidiennement en

temps normal et peuvent complètement déstabiliser les acteurs et leurs pratiques managériales. La réaction des individus face au stress peut être paralysante et complètement inappropriée face à la situation, la préparation psychologique et mentale fait à part entière partie de la préparation globale aux SSE. En temps normal, le raisonnement des individus circule à travers des règles, un cadre ordonné, maîtrisé, un environnement stable où il est plus facile d'établir des raisonnements logiques et peu biaisées.

Les crises induisent des phénomènes de « rupture créatrice » qui permettent de prendre les bonnes décisions face à des situations ne faisant pas partie du quotidien, mais qui passe par une acceptation de la non maîtrise totale de la situation, une acceptation à la surprise, à l'information incomplète, à l'incertitude, tout cela dans une temporalité plus ou moins rapide en fonction de la typologie de crise (temporalité plus longue dans le cadre de la gestion de la crise Covid par exemple, temporalité très courte dans le cas d'une cyberattaque).

Il faut donc apprendre à « changer de lunettes », à savoir se comporter face à l'imprévu, apprendre à penser l'impensable, ouvrir son esprit afin d'avoir la vision la plus claire possible dans un environnement particulièrement flou, transformer ses erreurs en opportunités et toujours partager l'information.

Même si certaines personnalités sont de base plus à l'aise que d'autres dans ce type de situation, il reste possible de se préparer et de s'améliorer en s'entraînant via des mises en situation, des exercices de gestion de crise, avec des simulations de cellule de crise. L'entraînement va permettre de mieux gérer le stress le jour venu, de s'entraîner à « penser différemment », à « passer en mode crise ».

La cellule de crise hospitalière (CCH) fait partie intégrante du processus de gestion de crise à l'hôpital. Elle ne doit pas être une entité « ad hoc » mais doit être préparée en amont et doit fonctionner en mode « REAC », c'est-à-dire faire preuve de Réactivité, Efficience, Adaptabilité et Cohésion »[21]. La notion de réactivité étant intimement reliée au facteur temps, particulièrement déterminant dans les conséquences de la crise, alliant un temps de réflexion et de concertation optimum, nécessaire pour éviter de tomber dans de la précipitation. L'efficience allie la gestion des ressources en fonction de l'objectif recherché. L'adaptabilité doit être inhérente au membres de la cellule de crise, afin que chaque acteur s'adapte aux paramètres de la situation en question et fasse preuve « d'une intelligence des situations ». La cohésion fait elle référence à la nécessité de « bâtir le groupe autour d'une confiance mutuelle », que « chacun accepte le jugement constructif de ses pairs pour faire progresser l'ensemble de l'équipe dans la résolution du problème ».

[21] Laurent Combalbert et Eric Delbecque, « La gestion de crise », 2018

La pratique, l'entraînement des acteurs, permet de travailler sur ces quatre points, et d'améliorer le fonctionnement général de la cellule de crise hospitalière. La cellule de crise englobe dans le même terme un lieu et une équipe organisée. Elle obéit à une démarche et à un schéma de projet pour la structure. Son objectif est de concevoir, décider, et coordonner les réponses à apporter à la situation de crise voire d'accompagner le processus de crise tout entier.

Les observations faites de l'observation des différentes cellules de crise au CHBA ont fait ressortir des points clés d'une bonne gestion de crise :

- Préciser pour chaque poste les points clés de sa fiche de mission
- Utiliser des moyens matériels adaptés (outils, salle de cellule de crise)
- Définir le ou les circuits de communication/d'information : circuits d'entrée de l'information en cellule de crise, circulation de l'information, et diffusion en interne
- Fixer les règles et circuits de validation des informations sortantes vers l'extérieur
- Organiser le circuit de la prise de décision
- Vérifier que les documents de crise sont à jour et que les outils sont fonctionnels

Ces différents points sont plus évidents à citer qu'à pleinement intégrer et réussir. En effet, ils sont primordiaux et doivent être travaillés et évalués lors d'entraînements de simulation de cellule de crise hospitalière car leur maîtrise est délicate et fluctuante, tout particulièrement pour les points 2 et 4.

Concernant l'utilisation de moyens matériels adaptés, il faut particulièrement souligner l'importance d'avoir une salle de crise qui permet d'accueillir les différents membres de la cellule sur un temps qui peut être long, dans un contexte de communications multiples, simultanées, permettant un partage de l'information rapide et qualitatif.

On peut par exemple citer les éléments suivants :

- La présence d'un grand tableau blanc, permettant d'y noter régulièrement le récapitulatif des points de situation. Chaque membre arrivant dans la salle pourra, sans rajouter de sollicitations, avoir face à lui le dernier point de situation avec tous les éléments essentiels d'une part mais surtout la même information et les mêmes éléments que les autres membres (la

communication orale est biaisée car elle peut contenir des erreurs et/ou une information incomplète)

- Une salle de crise avec un espace suffisant (en fonction du nombre des membres que va accueillir la salle de crise). Il faut noter que la cellule de crise détient un noyau de membres avec certains d'entre eux étant toujours présents en salle de crise, et d'autres faisant des allers-retours entre le terrain et la salle pour ensuite venir faire les remontées d'information par exemple. Plus il y aura de membres présents simultanément en cellule de crise, plus cela complexifiera la communication en son sein.
- Un ravitaillement régulier en eau, nourriture, crayons, supports papiers.
- Une aération possible de la salle de crise
- Une localisation stratégique de la salle de crise, afin que les acteurs faisant des aller-retours entre le terrain et la salle ne perdent pas trop de temps notamment. Mais aussi stratégique en termes de confidentialité, de passage, d'accessibilité.

Notons que même si ces points peuvent paraître plus anecdotiques que les autres, il n'en est rien. Ils conditionnent clairement le bon fonctionnement d'une cellule de crise et peuvent, à contrario, poser de vraies difficultés s'ils ne sont pas travaillés.

Ensuite, la composition de la cellule de crise et le rôle de chaque membre doivent être préalablement définis (dans le Plan Blanc) mais aussi ré-identifiés à chaque début de cellule de crise afin de poser le cadre de fonctionnement de la cellule et d'éviter le dépassement du cadre, des missions de chacun, pouvant donner lieu à des erreurs, des contre-décisions, des mauvaises interprétations, des problèmes de communication. Des « fiches de postes » détaillées peuvent être intéressantes à formaliser.

Ce que l'on peut appeler le « facteur humain » en cellule de crise est important à considérer car les comportements de chacun sont guidés et influencés par leurs émotions. Une situation de contrainte va entraîner des comportements inhabituels et imprévisibles. Comprendre les comportements humains les plus courants en cellule de crise en situation de stress pour mieux les intégrer est une clé pour améliorer la résilience et la préparation à la réponse. En effet, nos vies sont réglées par nos émotions, comme facteurs de survie et d'adaptation permettant à l'organisme de donner sens et valeur aux évènements et de s'y adapter. Il est donc nécessaire de comprendre leurs impacts dans le processus décisionnel.

Un point crucial et souvent peu perçu comme tel, est celui de la prise de note du relevé de décisions, ou tableau de suivi des actions ainsi que celui de main-courante. Le tableau de suivi des actions a pour objectif de synthétiser au temps T les décisions prises et principaux évènements, il doit être mis à jour régulièrement afin de permettre le suivi des décisions, et donne une vision commune et partagée de la situation comme base de point de situation. Cela peut être matérialisé par un tableau blanc, paperboard, outil numérique permettant le partage en temps réel avec les équipes opérationnelles. Il peut prendre la forme suivante :

Heure	Evènement	Décision/action	Suivi	Difficultés

Concernant la main-courante, elle assure la traçabilité et le suivi des actions, garantie la mémoire et la traçabilité des actions, des décisions et de la communication, permet lors des relèves d'avoir une vision globale de la crise et peut aussi être saisie par la justice. Le format le plus adapté est sûrement un fichier Excel partagé et projeté, imprimé avant chaque point de situation. Ci-dessous une trame possible de cette main-courante :

Heure	Expéditeurs	Destinataires	Information/Evènement	Actions	Bilans

Au sujet de l'animation de la cellule de crise, « *cette question est majeure, n'importe quel directeur de garde doit être capable d'animer une cellule de crise, au moins ses premières minutes et/ou heures, être capable de bien caractériser la situation, prendre la bonne décision, mettre autour de soi des expertises qui vont permettre de caractériser l'évènement le plus rapidement possible et de prendre les premières décisions de manière réactive.* » (P. COUTURIER, CHBA)

3.3.2 La rédaction d'un plan de communication de crise adapté

Lorsque survient une cyberattaque, un plan de communication doit être prêt, cela évitera d'une part de perdre du temps à le travailler dans l'urgence, mais aussi d'avoir une trame et une stratégie qui aura été préparée donc anticipée et réfléchie en amont, et qui sera donc objectivement décidée. Ce plan de communication fait partie intégrante d'une préparation à la gestion des risques. Les questions suivantes sont à se poser (cf schéma ci-dessous) :

- A qui communiquer ? Lister l'ensemble des acteurs à prévenir ou à ne pas oublier permet le jour J de ne pas passer côté de l'information d'un partenaire, ce qui pourrait être problématique.
- Quoi communiquer ? Les acteurs ne vont pas tous recevoir la même information, selon la politique du « need to know », il faut communiquer sur ce que les personnes doivent savoir à l'instant t, sans donner plus d'informations qui n'auraient pas d'utilité.
- Qui communique ? Dans les différents cas, ce sera souvent la Direction Générale qui sera le premier représentant de l'établissement et donc le premier interlocuteur pour communiquer. Il peut cependant être accompagné par d'autres acteurs, définis en fonction du type de crise subie : PCME, chef de service des urgences, Directeur de la communication, Directeur des systèmes d'information, Directeur Général adjoint…)
- Quand communiquer ? La temporalité de la diffusion de l'information a toute son importance. Ne pas communiquer trop vite ni trop tard, faire des points réguliers, la communication ne sera pas faite dans la même temporalité en fonction des différents acteurs non plus.

La communication, qu'elle soit interne (envers des professionnels de l'établissement) ou externe (envers tout acteur extérieur à l'établissement : population, presse...) est un élément vital à chaque étape de la réponse à une cyberattaque. Contrôler les flux de communication afin de s'assurer que la bonne information soit transmise par les bons émetteurs envers les bons destinataires et au bon moment est essentiel.

Le juste équilibre est à trouver entre la transparence et la protection. De plus, la communication trop rapide ou trop diffuse peut laisser place à des informations erronées, non vérifiées, ou qui peuvent entre temps évoluer et ne plus être d'actualité. Il faut aussi identifier les différentes parties prenantes qui auront besoin d'être informées individuellement, avec une communication personnalisée.

La gestion de l'information et de la communication, en temps de crise, est primordiale. La communication apparaît comme « *l'outil indispensable à la gestion d'une situation dégradée et donc à la protection d'une organisation* »[22]. Etablir un plan de communication permet de « *maîtriser les flux d'informations générés par l'entreprise en temps de crise* ».

Avoir un discours sincère, authentique est le meilleur moyen de réussir sa communication, tout en décidant d'adopter une communication plus ou moins exhaustive. Dans le cas d'une cyberattaque par exemple, la communication diffuse de la vulnérabilité de l'établissement peut-être un choix ayant des répercussions positives (peut susciter de l'aide de l'extérieur, une meilleure compréhension des difficultés de prise en charge de la part du grand public, une transparence appréciée) comme négatives (augmentation de la vulnérabilité pouvant donner lieu à une ou plusieurs autres attaques, peur de la part des professionnels, du grand public…). Chaque stratégie de communication peut avoir ses avantages et inconvénients et doit s'adapter à la situation de l'établissement au moment où il communique, l'important étant d'avoir une communication maîtrisée, décidée en amont et concertée avec les acteurs clés, donner les bonnes informations, et ne pas improviser sa communication.

En ce qui concerne le CHBA, une fois l'alerte reçue, il a tout de suite été convenu qu'aucune communication externe au-delà de l'ARS ne mentionnerait la notion de « cyber attaque » afin de ne pas augmenter la vulnérabilité de l'établissement et le risque d'être attaqués par d'autres hackeurs. Ainsi la terminologie « cybervigilance » a été choisie pour la communication interne. Cela a évité que la presse ne se saisisse du sujet comme elle a pu le faire pour le CHU de Rennes quelques mois après. « *Nous avons assez peu communiqué au fond, contrairement à d'autres établissements. Nous avons intégré l'idée que si nous étions discrets, nous aurions moins de risque d'augmenter notre vulnérabilité. Des dispositifs de virus non activés auraient pu être placés et activés à distance, nous craignions cela. Très peu de communication externe a été faite autour de la cyberattaque dont nous avons été victimes, nous avons fait profil bas, et nous ne regrettons pas d'avoir fait le choix d'une communication plus sobre.* » (P. COUTURIER, CHBA) « *La question suivante s'est rapidement posée : est-ce que l'on communique ? Nous avons pris le parti de ne pas utiliser le mot cyberattaque, nous ne voulions pas montrer notre fragilité à l'extérieur, c'était notre choix. L'idée était que cette communication soit axée vers la préparation des plans de continuité, que cela ait des vertus pédagogiques envers les agents*. » (V. JOUVET, CHBA)

La communication a donc été particulièrement maîtrisée tout en informant qu'une vigilance forte devait être de mise, en vue du contexte et permettait aussi de justifier le travail demandé autour des plans de continuité. « *Nous avons eu la stratégie d'une*

[22] Laurent Combalbert et Eric Delbecque

communication maîtrisée quasi immédiate. En termes de communication externe, nous avions la communication avec les tutelles mais nous n'avons pas souhaité communiquer avec la presse » (M-D NAEL, CHBA)

« *L'établissement a choisi de ne pas communiquer ou plutôt de communiquer sur une cyber vigilance. Tant que les investigations n'étaient pas conduites, c'était nécessaire* » (C. ALANIC, CHBA). La communication a ensuite permis de donner du sens aux mesures : plus d'accès au télétravail, plus d'accès à internet, plus de possibilité d'organiser des réunions Teams..

« *Je pense tout de même qu'une meilleure communication externe aurait permis d'informer les autres établissements bretons qui avaient entendu des bruits* » (C. ALANIC, CHBA)

Les autres établissements de la direction commune ont été informés mais par exemple, l'établissement public de santé mentale de St-Avé, membre du même GHT, n'a pas été immédiatement informé. Cela a été considéré comme une maladresse commise dans une situation d'urgence et de multiples sollicitations.

Il n'y a donc pas de stratégie de communication type applicable en toute situation. Il existe différentes possibilités de communiquer, chaque stratégie ayant ses avantages et ses inconvénients. Dans le cas d'une communication de crise liée à une attaque cyber d'un établissement de santé, chacun d'entre eux a décidé de communiquer de différentes manières, en lien avec le contexte de la situation et les objectifs de l'établissement. Le plus important est que la stratégie de communication de l'établissement soit une stratégie choisie, et non subie, cela suppose qu'elle soit anticipée, préparée, et considérée dès le départ comme un élément à acter pour la gestion de crise.

Conclusion

La menace cyber est un des plus grands défis de notre siècle. Les établissements de santé en sont devenus une cible privilégiée et les attaques cyber envers les hôpitaux ne cessent de s'accumuler depuis plusieurs années. L'ampleur du phénomène et les conséquences lourdes qu'il entraîne oblige aujourd'hui les établissements de santé à s'engager dans une démarche de préparation au risque cyber, souvent peu traitée jusqu'alors. Le concept de préparation s'entend de manière large et prend en compte non seulement la prévention du risque numérique via la maîtrise des systèmes d'information, mais aussi l'élaboration d'un plan blanc numérique décrivant les mesures activables en fonction de la nature, de l'ampleur et de la cinétique de l'incident numérique, identifiant les mesures à mettre en œuvre et la stratégie de l'établissement face à un incident numérique.

La construction de plans de continuité d'activité véritablement opérationnels et testés au sein des services de l'hôpital est inévitable et constitue le socle d'une bonne préparation. Cependant, le contexte actuel des hôpitaux condamnés à gérer l'urgence au quotidien, ne favorise généralement pas la priorisation de ces travaux pourtant bien identifiés comme essentiels. Le succès de cette préparation passe alors par un vrai travail d'acculturation au risque cyber, ainsi qu'à la gestion des risques de manière générale, en tentant de lever les freins existants, afin d'engager une démarche continue de gestion du risque. Un élargissement de cette prise de conscience à l'ensemble de l'équipe de Direction me semble impératif au même titre que les plans de sécurisation d'établissements.

La préparation est aussi complétée par des exercices, tests, simulations, permettant de tester les outils en place d'une part, et de former les différents acteurs d'autre part. Je saurai dans mes futures fonctions être vigilante quant à la prise en compte de cette nécessaire acculturation par l'ensemble des directions fonctionnelles, incluant aussi la Direction des affaires juridiques, la Direction des ressources humaines et des affaires médicales, la formation continue, voire les cursus de formation des IFSI/IFPS. Un travail de professionnalisation de la cellule de crise hospitalière (via des outils, des formations sur la gestion de crise...) permettra le cas échéant, d'avoir le maximum de clés en main pour faire face à la typologie de crise qui sera à gérer. En effet, le management de crise n'est pas une compétence naturelle mais bien une compétence à acquérir, facilitée par des aptitudes plus ou moins présentes, mais qui se travaillent de manière continue afin de favoriser la meilleure adaptabilité et agilité possible. Ces exercices de simulations de crises médico-administratives me projetteront également dans un management participatif.

Bibliographie

Ouvrage

COMBALBERT L., DELBECQUE E., « La gestion de crise », Que sais-je ?, Presses Universitaires de France, 2018

Articles de périodiques, revues

GROUPEMENT HOSPITALIER BROCELIANDE ATLANTIQUE, « B.A – BA magazine », 2023

HAMELIN C, CORDON S., « Retour d'expérience, CHU de Rouen confronté à une attaque en 2019 », Journal du droit de la santé et de l'assurance maladie (JDSAM), 2021

PARGUET J-F, « Etat de la menace cyber à mai 2021 », Journal du droit de la santé et de l'assurance maladie (JDSAM), 2021

CORDON S. « Le besoin grandissant de sécurisation des données médicales des établissements de santé et le cadre de développement des réponses apportées », Journal du droit de la santé et de l'assurance maladie (JDSAM), 2021

BARBERYE R., « L'hôpital public en danger », Gestion & Finances publiques, 2018

ZIZAR W., « Le coût total de la cyberattaque du CH de Dax s'est élevé à 2,3 millions d'euros (RSSI) », 2022

DE BRIANT L., « Cyberattaques contre les hôpitaux : la question n'est pas de savoir si cela va arriver, mais quand », 2023

Etudes, rapports, guides

MINISTERE DES SOLIDARITES ET DE LA SANTE, « Guide d'aide à la préparation et à la gestion des tensions hospitalières et des situations sanitaires exceptionnelles », 2019

MINISTERE DE LA SANTE ET DE LA PREVENTION, « Plan blanc numérique, établissements de santé, guide d'aide à la préparation », 2023

VAN DER LINDE C., « Appréhender dans sa globalité les rôles et attendus d'un cadre dans la planification et la gestion des tensions hospitalières et des situations sanitaires exceptionnelles et/ou de crise en établissement », 2022

CRYSALIDE, Retour d'expérience de l'exercice de crise au CHBA, 2023

ANSSI, « Mesures cyber préventives prioritaires », 2023

ANSSI, Guide « Anticiper et gérer sa communication de crise cyber », 2021

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

OBSERVATOIRE DES METIERS DE LA CYBERSECURITE, Enquête « L'attractivité et la représentation des métiers de la cybersécurité », 2022

HAS, « Prise en charge des situations sanitaires exceptionnelles selon le référentiel de certification », 2022

CENTRE FOR CYBER SECURITY BELGIUM, « Cybersécurité, guide de gestion des incidents », 2021

AGENCE DU NUMERIQUE EN SANTE, « Cybersécurité dans le secteur de la santé et du médico-social : une priorité nationale pour réussir la transformation numérique », 2021

INSTITUT DES ACTUAIRES, « Emergence du besoin en cyberassurance », 2017

Références juridiques

Articles L. 3131-1 du code de la santé publique

Article R. 3131-10 du code de la santé publique

Article D. 312-160 du code de l'action sociale et des familles

Liste des annexes

Annexe I : Grille d'entretien

GRILLE ENTRETIEN MEMOIRE :

Sujet : « *La préparation des établissements de santé aux phénomènes de cyber attaque : cas du CHBA* »

1) Présentez-vous (nom, fonction, lien avec le sujet..)

I) Vécu de la cyberattaque au CHBA :

2) Pouvez-vous me raconter en quelques mots comment vous avez vécu de votre position, l'évènement de cyberattaque au CHBA en décembre dernier ?

3) Quelle a été votre manière de gérer cette crise ? Quelle a été la stratégie de l'établissement ? Quels étaient les enjeux ?

4) Quelle stratégie de communication (interne et externe) a été choisie autour de cette crise ? quels enjeux existent en termes de communication autour de ce sujet ?

5) Quel a été l'accompagnement des tutelles à ce sujet ? A-t-il été suffisant ?

6) Les tutelles ont-elles organisé un ou plusieurs retours d'expérience ou autre forme d'échanges sur le sujet avec d'autres établissements du territoire ?

7) Pensez-vous que le CHBA était préparé à vivre cette cyberattaque ? Quel niveau de préparation avant la cyberattaque ?

II) Préparation au risque de cyberattaque :

8) Comment s'est organisée la préparation au risque cyber au CHBA ? Quelles difficultés rencontrées ? Menée d'emblée pour la direction commune ? groupement ? pourquoi ?

9) De quels appuis avez-vous pu bénéficier pour la préparation au risque cyber ? (Compétences RH en interne, appuis extérieurs…). De quels appuis le CHBA ne s'est pas encore saisi ?

10) Quelle a été la mobilisation des professionnels dans la préparation au risque cyber ? Comment le justifiez-vous ?

11) De manière plus générale, quels sont aujourd'hui les moyens mis en œuvre pour faire face au risque cyber pour le CHBA ? Est-ce suffisant selon vous ?

III) Autres

12) Selon vous, quelles sont les obligations aujourd'hui en termes de cybersécurité pour les établissements de santé ?

13) Pensez-vous que les établissements de santé ont tous conscience de leur vulnérabilité face à ce risque et l'impact conséquent d'une cyberattaque sur le fonctionnement de leur établissement ?

14) A votre avis, pourquoi les établissements de santé sont des cibles intéressantes pour les hackeurs ?

15) Selon vous, quelles sont les mesures permettant de prémunir un établissement de santé face au risque de cyber attaque ?

16) Quelles recommandations faire aux établissements de santé dans la préparation au risque ? dans la gestion du risque ?

17) Si c'était à refaire, que changeriez-vous dans la manière de gérer cette crise ?

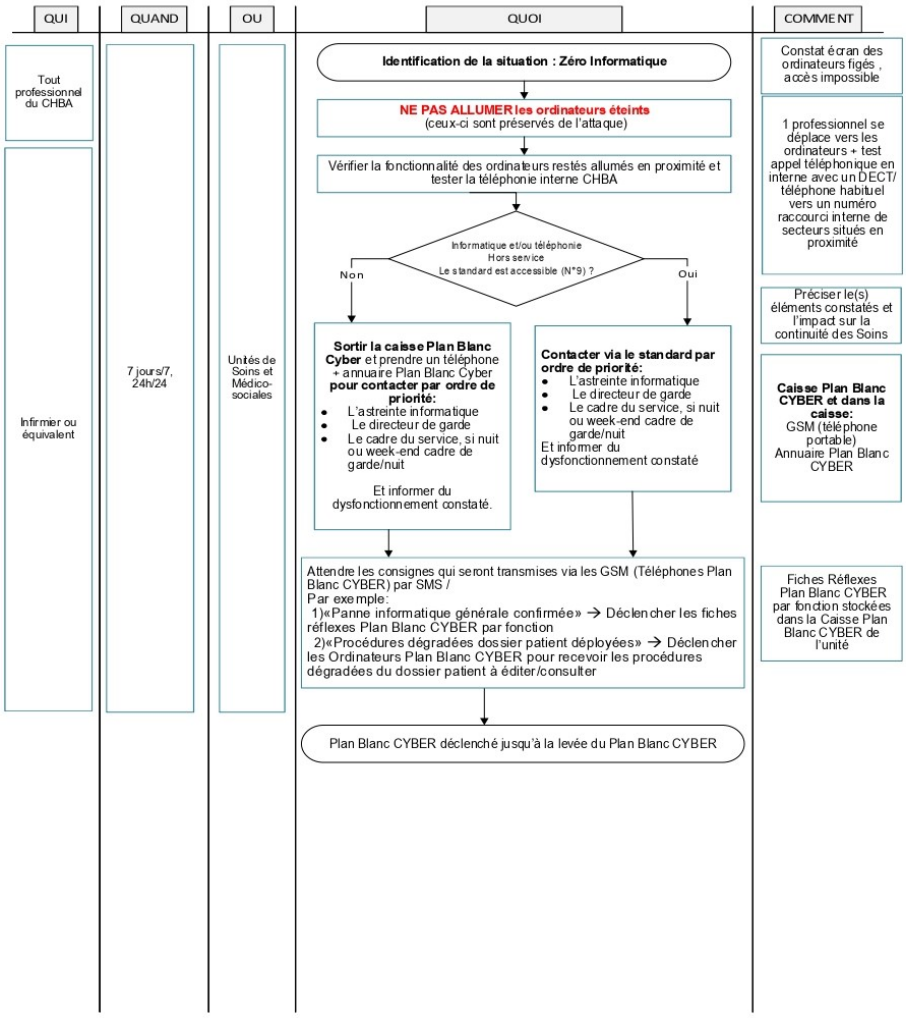
18) Autres éléments à partager sur le sujet ?

Annexe II : Procédure de déclenchement du plan blanc dans les unités de soins et médico-techniques

BROCÉLIANDE ATLANTIQUE GROUPEMENT HOSPITALIER Vannes - Auray	**Déclencher le Plan Blanc CYBER** **Unités de soins et médico techniques** **Vérification de la caisse, et outils** **« Plan Blanc CYBER »**	V 2 SSE 096 - V1 Date application : 27/02/2023 Nbre de pages : 1/5

1. Objet	2. Domaine d'application
Cette procédure a pour objet de définir la conduite à tenir pour les professionnels présents dans les unités de soins, en situation d'inaccessibilité du réseau téléphonique et ou informatique pouvant aller jusqu'au black-out total.	Cette procédure concerne et s'applique à tous les professionnels des unités de soins, 7 jours sur 7 et 24h/24
3. Définitions et abréviations	**4. Responsabilités**
	IDE, AS, Cadre de santé.

5. Contenu



Mots clés : Attaque, Attack, informatique, téléphonie, téléphone, panne, caisse, boite, kit, black-out, portables

5.1. Conduite à tenir

Etape	Lieu (Où)	Acteur (Qui)	Action (Quoi et pourquoi)	Relation (Comment)
1	Tous services	Tout professionnel	**Identifie la situation** : **Zéro informatique** dans le secteur de soins et dans les unités à proximité : écran figé bleu ou autre, accès impossible aux outils de travail.	Se déplacer pour objectiver auprès des collègues présents
2	Tous services	Tout professionnel	**NE PAS ALLUMER LES ORDINATEURS QUI SONT ETEINTS.** Se déplacer vers un autre ordinateur qui est resté allumé dans l'unité ou à proximité : situation identique ou non ?	
3	CHBA	Tous	Vérifie la fonctionnalité de la téléphonie dans le service	Tester l'appel vers un autre téléphone en interne CHBA et externe (Sur un 06 ...) si le poste le permet habituellement
4	CHBA	IDE	**Informatique Hors service - téléphonie est opérationnelle :** **Contacter par ordre de priorité** 1. L'astreinte informatique 2. Ou Le directeur de garde 3. Ou Le cadre du service, si nuit ou week-end cadre de garde/nuit : 4. Ou sur les lignes de secours du standard Et informer de la situation : • Informatique : constat des ordinateurs du service (par exemple écran bleu fixe, préciser le message affiché...) • Téléphonie : fonctionnelle en appels internes et/ou externes	Numéro du standard : « 9 » qui transfère l'appel.
5	CHBA	IDE	**Si la téléphonie n'est pas opérationnelle : aller chercher le téléphone GSM « Plan Blanc CYBER » dans la caisse « plan blanc CYBER »** Et se référer à la fiche réflexe IDE Transmettre les éléments observés concernant l' informatique et la téléphonie	Annuaire des GSM Plan Blanc Cyber
6	CHBA	IDE	**GSM Plan Blanc CYBER : Réception d'un SMS de déclenchement par le Directeur de Garde du Plan Blanc CYBER**	GSM Plan Blanc CYBER

6. Vérification des Outils Plan Blanc CYBER

6.1 - La caisse « Plan Blanc CYBER »

Chaque service de soins et médicotechniques est doté d'une caisse « Plan Blanc CYBER », adaptée à l'activité de l'unité. Le contenu de la caisse est défini. La caisse est scellée afin de garantir sa complétude en cas de déclenchement du Plan Blanc CYBER.

La vérification du contenu de la caisse est à réaliser :

- 2 fois / an :
  - En début d'année
  - En milieu d'année
- 1 fois par l'équipe de jour **et** la seconde par l'équipe de nuit, en lien avec le cadre de nuit.

La vérification est à réaliser systématiquement dès lors qu'elle a été utilisée en situation réelle ou en situation d'exercice/entraînement.

La traçabilité de la vérification de la caisse est assurée sur le support « Check-list des outils Plan Blanc Cyber ».
La fiche de vérification est glissée dans une pochette transparente et fixée à 1 des 2 scellés qui ferment la caisse.

6.2 - Vérification des GSM (téléphones portables) Plan Blanc CYBER stockés dans la caisse Plan Blanc Cyber du service

2 fois par an, vérifier :

- La présence des téléphones portables (et chargeur) à partir de l'annuaire Plan Blanc CYBER pour le service
- La charge de la batterie, si besoin mettre en charge maximum 1/2h

6.3 - Vérification du/des ordinateur(s) portables Plan Blanc CYBER stocké(s) dans la caisse Plan Blanc Cyber

2 fois par an, vérifier :

- La présence de l'ordinateur portable avec 1 clé 4G : 1 par service (ou pour les services de + de 40 lits = 2 ordinateurs), avec un câble pour branchement sur l'imprimante dédiée « Plan Blanc CYBER » destinée à éditer les procédures dégradées du dossier patient (sauvegardes Pdf des prescriptions médicamenteuses et observations médicales).

En cas d'écart, prévenir sans délai la DSIT (Direction des systèmes d'information Territoriale) via la hot line informatique et faire une Fiche d'Evénement Indesirable pour régulariser.

7. Utilisation des outils stockés dans la caisse Plan Blanc Cyber

7.1 Caisse Plan Blanc Cyber

La caisse scellée est accessible au niveau d'un bureau infirmier N°1 (ou équivalent).
Le contenu de la caisse permet de faire face à une panne informatique et/ou téléphonie générale. En cas de nécessité, il convient de retirer les scellés pour l'ouvrir.

7.2 Téléphones Portables Plan Blanc Cyber en lien avec l'annuaire Plan Blanc Cyber

Ces téléphones sont identifiés par fonction (IDE, cadre, AMA, Médecin ...) et par service. **Il est impératif de respecter la répartition prévue en lien avec l'annuaire Plan Blanc Cyber. L'IDE secteur 1 utilise le téléphone lié à sa fonction et son poste de travail** le jour concerné.

7.3 Annuaire des téléphones portables - GSM Plan Blanc Cyber

Un annuaire permet de contacter les professionnels de l'établissement en situation de Plan Blanc Cyber.

7.4 Ordinateur Plan Blanc CYBER avec clé 4G et câble imprimante / secteurs couverts par la 4G

Stocké dans la caisse « Plan Blanc CYBER », il permet en cas de déclenchement du Plan Blanc CYBER par le directeur de garde/cellule de crise, de recevoir automatiquement les procédures dégradées du dossier patient au format Pdf (Pas d'accès au logiciel dossier patient) et de les éditer.

Le mode opératoire pour accéder aux procédures dégradées du dossier patient est présent avec l'ordinateur Plan Blanc CYBER, il explique comment réaliser l'édition papier du dossier patient.

- **Impression en 1 exemplaires des prescriptions de médicaments :**

    - Traçabilité des soins pour 24 heures

Les IDE éditeront le support des prescriptions de médicaments (version imprimable) et documenteront les administrations médicamenteuses réalisées sur le support papier.
Toute nouvelle prescription sera réalisée sur le support de prescription papier vierge, support présent dans le kit dossier patient Plan Blanc Cyber stocké dans la caisse plan Blanc Cyber.

Pour les secteurs non couverts par le réseau 4G, l'équipe de la Direction informatique livrera dans les unités de soins concernées, un (ou des) ordinateur(s) avec les procédures dégradées du Dossier Patient (prescriptions médicaments, observations médicales et RDV) au format Pdf.

7.4 Cahier de main courante

Il est destiné à noter tous les éléments marquants du service concernant la prise en charge des patients en terme d'organisation, éléments à faire remonter à la Cellule de crise par l'encadrement paramédical/médical.
Chaque jour, une nouvelle page est créée, sont notés :

- La date du jour/ heure
- La signature de l'auteur
- Le/les événements marquants

Il est conservé dans le bureau IDE du secteur 1 ou équivalent. Il est consulté par l'encadrement qui transmettra les éléments pertinents à la cellule de crise.

7.5 Ramettes de papier blanc

Les 2 Ramettes de papier sont destinées à l'édition des prescriptions médicamenteuses pour les 24 premières heures.

7.6 Dossier patient papier

Un kit dossier patient est présent dans une pochette cartonnée.

Comment utiliser le dossier patient papier « standard » : certains services bénéficient d'un dossier patient spécifique (exemple la Réanimation adulte, Pédiatrie, Dialyse…)

Dans la Caisse Plan Blanc Cyber, il convient de prendre une pochette avec le kit complet (Fiche d'identification du patient, Désignation de la personne de confiance, autonomie, macrocible d'entrée, transmissions ciblées, observations médicales, prescriptions des examens complémentaires, Fiche de traçabilité des paramètres médicaux, diagramme de soins, fiche de liaison).

1. Mettre un dossier papier dans chaque classeur/patient par N° de lit
2. Coller sur chaque document 1 étiquette d'identification du patient ou à défaut une étiquette comprenant : nom de naissance + nom d'usage + prénom + date de naissance sur chaque recto et verso.

Consignes à respecter pour tracer:
Utiliser des crayons bleus pour les IDE, interdiction d'écrire au crayon gris.
Le correcteur (blanco, étiquette…) est interdit. L'erreur est barrée et signée.

Les abréviations sont fortement déconseillées (surtout dans la macrocible).

Mots clés : Attaque, Attack, informatique, téléphonie, téléphone, panne, caisse, boite, kit, black-out, portables

Les informations sont horodatées ainsi que l'identification claire et lisible du professionnel et sa fonction.

Les écrits sont continus. Il ne faut pas laisser de ligne entre chaque information.

Sur les feuilles de paramètres médicaux : la tension est écrite en noire, la température en bleue, le pouls en rouge et les urines en vert.

Tout professionnel est responsable de ses actes et de ses écrits.
Il doit donc en assurer la traçabilité avant de quitter son poste de travail.

7.7 Fiche reflexe de demande d'examen, de commandes et d'intervention

Tous les circuits habituels sont impactés, il convient de se référer à la fiche reflexe afin d'assurer les demandes d'examens, de commandes et de livraison.

7.8 Fiche de mouvement

Il s'agit d'avoir un état des lieux des patients présents dans l'unité.

7.9 Plan Blanc - BILAN des patients présents et orientations – à renseigner par le médecin

Il s'agit d'un document permettant au médecin de recenser les patients présents qui pourront rester hospitalisés et les perspectives de patients à transférer.

8. Documents associés

- Check List des outils « Plan Blanc CYBER »
- Documents contenus dans la caisse Plan Blanc CYBER

9. Suivi des versions

Version	Date	Nature des modifications
V1	Février 2023	Création

10. Circuit de validation

Rédaction	Validation	Approbation
Noms : Mme BETROM, Mme TECHER Fonctions : Cadres Supérieurs de santé Date : 27/02/2023 Signature ***Signé***	Noms : Mme DERCHE Fonctions : Coordonnatrice Générale des Soins Date : 27/02/2023 Signature ***Signé***	Nom : Mme NAEL Fonction : Directrice des Projets, de la Qualité et de la Gestion Des Risques Date : 27/02/2023 Signature ***Signé***

Annexe III : Check-list des outils dans les unités de soins en cas de plan blanc cyber

BROCÉLIANDE ATLANTIQUE GROUPEMENT HOSPITALIER Vannes - Auray	**Check List des outils dans les Unités de soins « Plan Blanc CYBER »** (PB Cyber) **Traçabilité des vérifications de la caisse / GSM(portables) / PC sécurisé**	V 4 SSE 097 - V1 Date application : 21/02/2023 Nbre de pages : 1/2

Service : .....
Suivi 2 fois/an (début et milieu d'année) **: Caisse Plan Blanc CYBER présente, complète et scellée.**

Dates des vérifications	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..
GSM- Téléphones PB Cyber (présents cf nombre dans l'annuaire, chargés et testés par un appel sur autre portable externe) → Nombre dans le service :*à préciser*.....									
Ordinateur Portable PB Cyber (avec cable électrique) + Clé 4G + câble imprimante PB Cyber présents. nombre :.....									
Caisse PLAN BLANC Cyber									
1 Annuaire avec numéros GSM plan blanc CYBER									
Nombre de dossiers patient papier (1 dossier par lit dans le service plus, 5 d'avance).									
1 Fiche reflexe IDE									
1 Fiche reflexe médecin									
Fiches « Bilan des patients présents et orientation »									
Formulaires de gestion des mouvements									
1 Cahier « main courante » pour les transmissions									
2 Ramettes de papier vierge									
1 bon de commande reprographie									

Validation : Direction des Soins, Février 2023

BROCÉLIANDE ATLANTIQUE GROUPEMENT HOSPITALIER Vannes - Auray	**Check List des outils dans les Unités de soins « Plan Blanc CYBER »** (PB Cyber) **Traçabilité des vérifications de la caisse / GSM(portables) / PC sécurisé**	V 4 SSE 097 - V1 Date application : 21/02/2023 Nbre de pages : 2/2

Dates des vérifications	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..	…./…../20..
1 Fiche reflexe de demande d'examen, de commandes et d'intervention									
Fiches de transmission rééducation (R60)									
5 Demandes ORIS (SSR)									
N° des 2 scellés posés	1- 2-	1- 2-	1- 2-	1- 2-	1- 2-	1- 2-	1- 2-	1- 2-	1- 2-
Identité+fonction+ Signature du professionnel qui a réalisé la vérification									

NB : s'il manque des GSM et/ou PC au moment des vérifications, le professionnel qui vérifie, rédige une Fiche d'Evenement Indésirable systématiquement.

Validation : Direction des Soins, Février 2023

HEURTIN	Laura	Octobre 2023

Directeur d'hôpital

2022-2023

La préparation des établissements de santé aux phénomènes de cyberattaques : cas du centre hospitalier Bretagne Atlantique

PARTENARIAT UNIVERSITAIRE : RAS

Résumé **:**

La menace cyber est un des plus grands défis de notre siècle. Les établissements de santé en sont devenus une cible privilégiée et les attaques cyber envers les hôpitaux ne cessent de s'accumuler depuis plusieurs années. L'ampleur du phénomène et les conséquences lourdes qu'il entraîne oblige aujourd'hui les établissements de santé à s'engager dans une démarche de préparation au risque cyber, souvent peu traitée jusqu'alors. Le concept de préparation s'entend de manière large et prend en compte non seulement la prévention du risque numérique via la maîtrise des systèmes d'information, mais aussi l'élaboration d'un plan blanc numérique décrivant les mesures activables en fonction de la nature, de l'ampleur et de la cinétique de l'incident numérique, identifiant les mesures à mettre en œuvre et la stratégie de l'établissement face à un incident numérique.

La construction de plans de continuité d'activité véritablement opérationnels et testés au sein des services de l'hôpital est inévitable et constitue le socle d'une bonne préparation. Cependant, le contexte actuel des hôpitaux condamnés à gérer l'urgence au quotidien, ne favorise généralement pas la priorisation de ces travaux pourtant bien identifiés comme essentiels. Le succès de cette préparation passe alors par un vrai travail d'acculturation au risque cyber, ainsi qu'à la gestion des risques de manière générale, en tentant de lever les freins existants, afin d'engager une démarche continue de gestion du risque.

La préparation est aussi complétée par des exercices, tests, simulations, permettant de tester les outils en place d'une part, et de former les différents acteurs d'autre part. Un travail de professionnalisation de la cellule de crise hospitalière (via des outils, des formations sur la gestion de crise...) permettra le cas échéant, d'avoir le maximum de clés en main pour faire face à la typologie de crise qui sera à gérer. En effet, le management de crise n'est pas une compétence naturelle mais bien une compétence à acquérir, facilitée par des aptitudes plus ou moins présentes, mais qui se travaillent de manière continue afin de favoriser la meilleure adaptabilité et agilité possible.

Mots clés **:**

Cyberattaque, plan de continuité d'activité, cybersécurité, cybervigilance, crise, CH, système d'information, cellule de crise, management, gestion des risques

L'Ecole des Hautes Etudes en Santé Publique n'entend donner aucune approbation ni improbation aux opinions émises dans les mémoires : ces opinions doivent être considérées comme propres à leurs auteurs.