Filière Directeur d'Hôpital

Promotion : **2023 - 2024**

Date du Jury : **Octobre 2024**

Cyberattaque, cyber-résilience et plans de continuité d'activité : Comment permettre à l'hôpital de continuer à opérer dès les heures qui suivent une cyberattaque

Hugo LE JALU

Remerciements

Je souhaite remercier Edith Benmansour, directrice générale du groupe hospitalier universitaire, pour sa confiance et pour m'avoir confié un dossier ambitieux et exigeant, que celui de la rédaction de plans de continuité d'activité pour son établissement. Sa vision, sa connaissance très fine des dossiers et de son établissement ont été une source d'inspiration.

Je souhaite également particulièrement remercier mon maître de stage, Fabien Gourdon, Directeur chargé des Affaires générales et Directeur chargé des Usagers, Risques, Crise et de la Qualité, pour sa bienveillance, son enthousiasme, sa gentillesse et sa disponibilité. Je lui suis très reconnaissant pour ses conseils et recommandations, qu'il m'a transmis en toute franchise et transparence. Ses avis éclairés ont enrichi mon expérience.

Je tiens aussi à remercier l'ensemble de l'équipe de direction, et plus particulièrement tous les directeurs avec lesquels j'ai pu collaborer directement, qui m'ont permis aussi bien de nourrir ce mémoire que de m'épanouir lors de mon stage.

Je remercie également toutes les équipes que j'ai pu rencontrer dans les services, qui m'ont accordé leur confiance et ont su se mobiliser pour se préparer en cas de cyberattaque, et qui ont su m'apporter un regard franc sur mais également nourrir ma réflexion lors de la rédaction de ce mémoire.

Plus généralement, je remercie toutes les personnes que j'ai pu rencontrer et qui se sont toujours montrées ouvertes et aidantes, contribuant ainsi de près ou de loin à la réflexion que représente ce travail.

Sommaire

Ps : mettre à jour via la touche F9

Liste des sigles utilisés

ANSSI : Agence nationale de la sécurité des systèmes d'information

ANS : Agence du numérique en santé

AP-HP : Assistance publique – hôpitaux de Paris

AP-HM : Assistance publique – hôpitaux de Marseille

BIA : Bilan d'impact d'activité

CERT : Computer Emergency Response Team

CRRC : Centre Régional de Ressources Cybersécurité

CH : Centre hospitalier

CHU : Centre hospitalier universitaire

DDoS : Distributed Denial of Service (en français : (attaque par) déni de service)

DGOS : Direction générale de l'offre de soins

DMP : Dossier Médical Partagé

ES : établissement sanitaire

GRADeS : Groupement Régional d'Appui au Développement de la e-Santé

HAS : Haute autorité de santé

HCL : Hopitaux civils de Lyon

MCO : Médecine, chirurgie, obstétrique

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

PCA : Plan de continuité d'activité

PCI : Plan de continuité informatique

PCRA : Plan de continuité et de reprise d'activité (*désignant alors le document cadre*)

PRA : Plan de reprise d'activité

PCI : Plan de reprise informatique

Introduction

À l'occasion des Jeux Olympiques de Paris 2024, l'AP-HP (Assistance Publique - Hôpitaux de Paris) met en place des Plans de Continuité et de Reprise d'Activité (PCRA) pour faire face à l'augmentation du risque de cyberattaque. Ce risque, déjà croissant chaque année, devient particulièrement préoccupant avec la tenue de cet événement international.

Les éditions précédentes des Jeux Olympiques ont été marquées par une recrudescence des cyberattaques : 200 millions de tentatives aux JO de Londres, 500 millions à ceux de Rio, et plus de 4 milliards de cyber incidents au Japon. Les estimations prévoyaient une multiplication par dix de ce type d'incidents en raison d'un contexte international tendu et des récentes attaques visant des établissements de santé et d'autres institutions publiques.

Les Jeux Olympiques de Paris ont donc représenté une menace significative pour les structures publiques, notamment pour les établissements de santé. Ces derniers, souvent moins bien préparés, sont des cibles attrayantes pour les cybercriminels en raison des données sensibles qu'ils manipulent. Toutefois, cet événement offre également une opportunité unique de mobiliser tous les acteurs de l'hôpital autour de la création de plans de continuité d'activité, avec une échéance claire : la cérémonie d'ouverture des JO.

La littérature sur les mesures de protection et de résilience des systèmes d'information avant une cyberattaque est abondante. Elle traite également de la sensibilisation et de la préparation des acteurs de l'hôpital public. En revanche, les méthodes de mise en place d'un Plan de Continuité d'Activité sont moins détaillées, préconisant la préparation d'un plan adapté à chaque scénario d'attaque ce qui se révèle en pratique impossible. Elle est quasi inexistante sur le contenu concret des PCA et sur les moyens d'assurer la continuité de l'activité hospitalière en cas de cyberattaque. Lorsqu'elle aborde ce sujet, la littérature se focalise généralement sur le pilotage de la continuité des soins par l'ARS et le recours au SAMU et aux établissements du territoire.

Ces solutions ne sont pas transposables à l'AP-HP, dont l'interconnexion des systèmes d'information et la position quasi monopolistique dans l'offre hospitalière de la région Île-de-France (avec 75 % des lits MCO) font craindre un arrêt de la majeure partie de l'offre de santé de recours et d'expertise en cas de cyberattaque totale sur l'établissement. Au vu de ce constat, le recours aux autres établissements du territoire apporterait une aide limitée, d'autant que certaines activités ne sont exercées que par l'AP-HP. Il en va de même pour bon nombre de centres hospitaliers de taille importante, pour les CHU et en particulier pour des établissements comme l'AP-HM ou les HCL.

Afin de faire face à la menace que représentent les cyberattaques, l'AP-HP souhaite se doter de PCRA pour l'ensemble de ses services d'ici janvier 2026. Une de mes missions en stage long au sein des Hôpitaux Universitaires Henri-Mondor consistait à concevoir des plans de continuité d'activité pour maintenir un haut niveau d'activité dans des services critiques avant les JO de Paris. La poursuite de cette mission et sa concrétisation m'ont amené à questionner l'adéquation de la documentation avec les besoins stratégiques, organisationnels et opérationnels nécessaires à la mise en place et la mise en œuvre de PCA.

Au regard de ces éléments, ce mémoire propose de répondre à la question suivante : Quelle stratégie adopter pour construire des plans de continuité d'activité opérationnels permettant aux services de maintenir un haut niveau d'activité dans un temps contraint ?

Fruit d'une réflexion professionnelle menée tout au long de la préparation de plans de continuité d'activité en cas de cyberattaque, ce travail s'appuie sur la rencontre de nombreux professionnels de différents établissements, la consultation extensive des documents issus des autorités de tutelle et des organismes spécialisés en santé numérique et cybersécurité, ainsi que de la consultation de documents mis en place par différents établissements et la participations à des webinaires et journées dédiées à ce sujet. Ces éléments sont détaillés dans la méthodologie qui suit.

Afin de répondre à cette question il conviendra d'abord d'exposer et de caractériser la menace à laquelle les hôpitaux font face, et de présenter s'ils existent, les dispositifs et actions préconisés voire mis en place par les autorités de tutelles pour y répondre. Il conviendra également de présenter l'état de l'art de ces défenses et leurs éventuelles limites. Dans un deuxième temps face à la difficulté de réaliser en temps et ressources contraints un travail inédit, le présent travail propose une méthodologie afin d'aboutir à la création de premiers PCA. Enfin, ce mémoire s'achève sur des propositions opérationnelles.

Méthodologie

Le travail qui suit s'appuie sur une extension et une généralisation des processus qui ont menée à la création de premiers PCA pour l'établissement où j'ai réalisé mon stage de direction. Comme précisé en introduction, l'AP-HP a en effet pour but de mettre en place des PCA dans l'ensemble des services d'ici à janvier 2026. Cependant face aux risques de voir les cyberattaques s'intensifier de manière colossale à l'occasion des Jeux Olympiques de Paris a conduit mon établissement de stage à vouloir se doter de PCA en amont de leur

tenue. J'ai donc dû mener ce travail en temps contraint et en avance de phase par rapport aux autres établissements de l'AP-HP qui ont pu rejoindre l'initiative par la suite.

Cette expérience m'a amené à aborder ce sujet avec de nombreux professionnels, au sein de mon établissement de stage, mais également à l'extérieur. Ces prises de contacts ont été précieuses à la réalisation de ce mémoire, en abordant à la fois des aspects pratiques et concrets lors de la mission qui m'était confié, mais aussi dans un second temps afin de prendre de recul pour proposer une approche généraliste et une réflexion globale.

Ce mémoire est également bâti sur la consultation des documents relatifs au sujet de la cybersécurité, de la cyber-résilience ou des PCA directement, produit par la DGOS, l'ANSSI, l'ANS, et parfois certaines ARS, Cert, ou GRADeS, qui proposent essentiellement un cadre théorique et des pistes de réflexion, et parfois quelques productions à visée plus opérationnelle et qui ont pu être éprouvés par un certain nombre de mes interlocuteurs.

Il est également le fruit d'échanges et d'entretiens avec des experts du domaine, acteurs ou non du monde hospitalier, rencontrés à l'occasion de webinaires, conférences ou journées organisées autour du sujet des cyberattaques pour les établissements sanitaires. Ces échanges constituent la première source de recherche, la littérature académique ou scientifique étant relativement limitée concernant des éléments qui permettrait d'irriguer un document aussi opérationnel qu'un PCA.

1 Les établissements sanitaires font face à un risque accru de cyberattaque

Les innovations technologiques ont transformé de manière radicale, en l'espace de quelques décennies, le secteur de la santé et en particulier les hôpitaux publics, où l'informatique occupe désormais une place centrale. Cependant, ce recours croissant à l'informatique et à la dématérialisation expose également ces établissements à de nouvelles menaces, parmi lesquelles les cyberattaques se distinguent par leur gravité et leur potentiel destructeur. Ce premier chapitre a pour objectif de présenter l'état de la menace cyber et les efforts engagés pour renforcer les défenses des hôpitaux, mais également d'en montrer les limites.

1.1 L'accroissement du risque de cyberattaque a conduit à renforcer les défenses des hôpitaux

1.1.1 Anecdotiques avant les années 2010, les cyberattaques se sont peu à peu professionnalisées et spécialisées et se sont multipliées ces dernières années

L'Agence nationale de la sécurité des systèmes d'information, autorité nationale en matière de cybersécurité et de cyberdéfense définit la cyberattaque comme : « Ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. » Plus précisément, l'ANSSI définit quatre grands types de motifs aux cyberattaques : la cybercriminalité à visée lucrative, l'espionnage, la déstabilisation et le sabotage.

Concernant les hôpitaux publics, la plupart des attaques ont une visée lucrative, avec notamment des vols de données dans le but de les revendre, mais d'autres types d'attaques à but purement déstabilisateur ne sont pas à écarter.

Une cyberattaque peut donc être définie comme toute action malveillante visant à compromettre la confidentialité, l'intégrité ou la disponibilité des systèmes d'information d'une organisation. Concrètement, ces attaques peuvent utiliser différents vecteurs, notamment des logiciels malveillants (*malware*), des rançongiciels (*ransomware*), des techniques de *phishing* (hameçonnage ou encore filoutage en français), ou encore les attaques par déni de service distribué (DDoS).

Principales Formes de Cyberattaques

Logiciels malveillants (*Malware*)

Les logiciels malveillants, ou malware, désignent tout programme ou code nuisible conçu pour infiltrer, endommager, ou prendre le contrôle d'un système informatique sans le consentement de l'utilisateur.

Rançongiciel (*Ransomware*)

Le rançongiciel, ou ransomware, est un programme chiffre les données d'un système ou bloque l'accès à ce dernier, puis exige une rançon en échange de la clé de déchiffrement ou de la restauration de l'accès. Ces attaques sont particulièrement dévastatrices pour les organisations où l'accès aux données est vital, et vise donc particulièrement les hôpitaux.

Hameçonnage (*Phishing*)

Le *phishing* est une technique d'escroquerie en ligne où les attaquants se font passer pour une entité légitime, généralement par le biais de courriels ou de sites web falsifiés, afin de tromper les utilisateurs et les inciter à divulguer des informations sensibles, telles que des identifiants de connexion, des numéros de carte bancaire, ou d'autres données personnelles.

Attaques par déni de service distribué (DDoS)

Les attaques par déni de service distribué (ou DDoS) consistent à inonder un système, un serveur ou un réseau de demandes simultanées provenant de multiples sources compromises, souvent un botnet, pour saturer les ressources de la cible. L'objectif est de rendre un service indisponible en interrompant le fonctionnement normal du site ou du réseau visé, causant ainsi des pertes financières et opérationnelles considérables.

Il est difficile d'identifier avec certitude le début des cyberattaques sur les hôpitaux, notamment en raison de l'instauration tardive d'un mécanisme de signalement des incidents cyber à caractère obligatoire au 1er octobre 2017, en application de l'article 110 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Néanmoins, les premières cyberattaques visant des établissements sanitaires ont eu lieu après le début des années 2010, mais restaient alors très circonscrite et largement le fait d'amateurs. La première attaque d'ampleur envers un hôpital avec paralysie de son système d'information

visant le Hollywood Presbyterian Medical Center, situé à Los Angeles aux Etats-Unis, ne date que de 2016 et marque un tournant dans le domaine.
L'année suivante, la DGOS publiait un « Mémento DGOS à l'usage du directeur d'établissement de santé, connaître vos risques pour mieux y faire face » dans lequel les exemples de risque de déstabilisation des établissements du système de santé ne duraient que quelques jours, pour des dégâts estimés entre 10 000 et 50 000 euros, essentiellement en perte de productivité.
Depuis, la situation est largement différente, avec une recrudescence des cyberattaques de grande envergure depuis 2019 et l'attaque du CHU de Rouen, considérée comme la première attaque d'ampleur en France.

La création en 2017 de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social, sous l'égide de l'Agence du numérique en santé, permet de mesurer, au moins partiellement, l'essor des cyberattaques. Ce comptage reste partiel dans la mesure où certains établissements ne déclarent pas ces incidents.

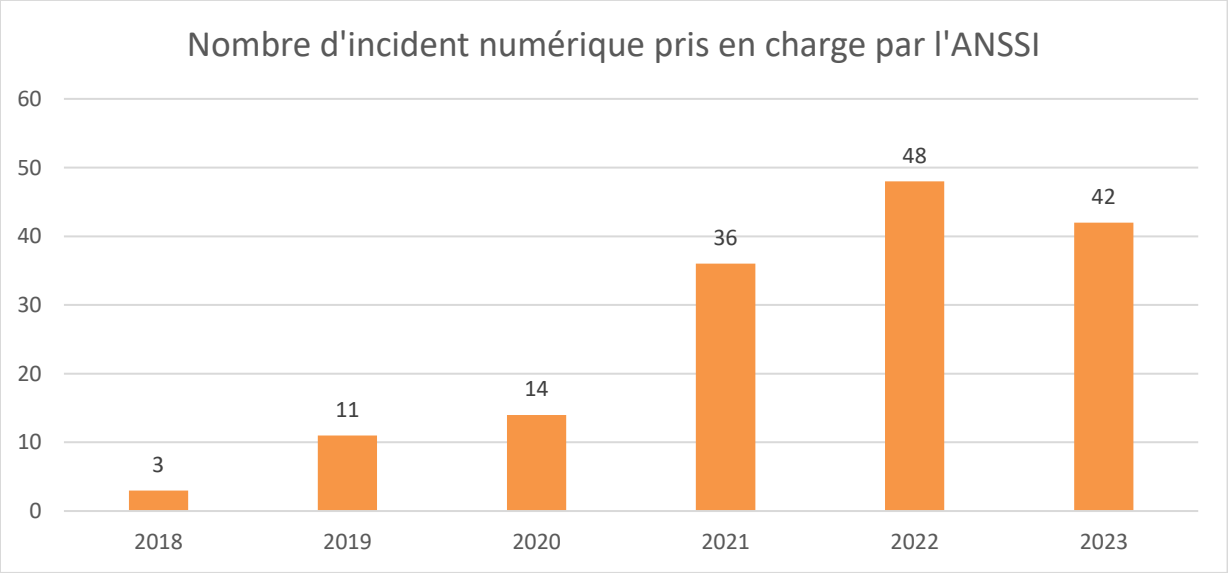

Figure 1 – Evolution du nombre de signalement d'incidents numériques pris en charge par l'ANSSI assimilables à des cyberattaques (l'ANSSI intervient lorsque les ressources de l'établissement sont débordées et ne peuvent effectuer seules le diagnostic de l'incident, supposant une attaque d'ampleur) – Source : données compilées issues des rapports 2018 à 2023 de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé

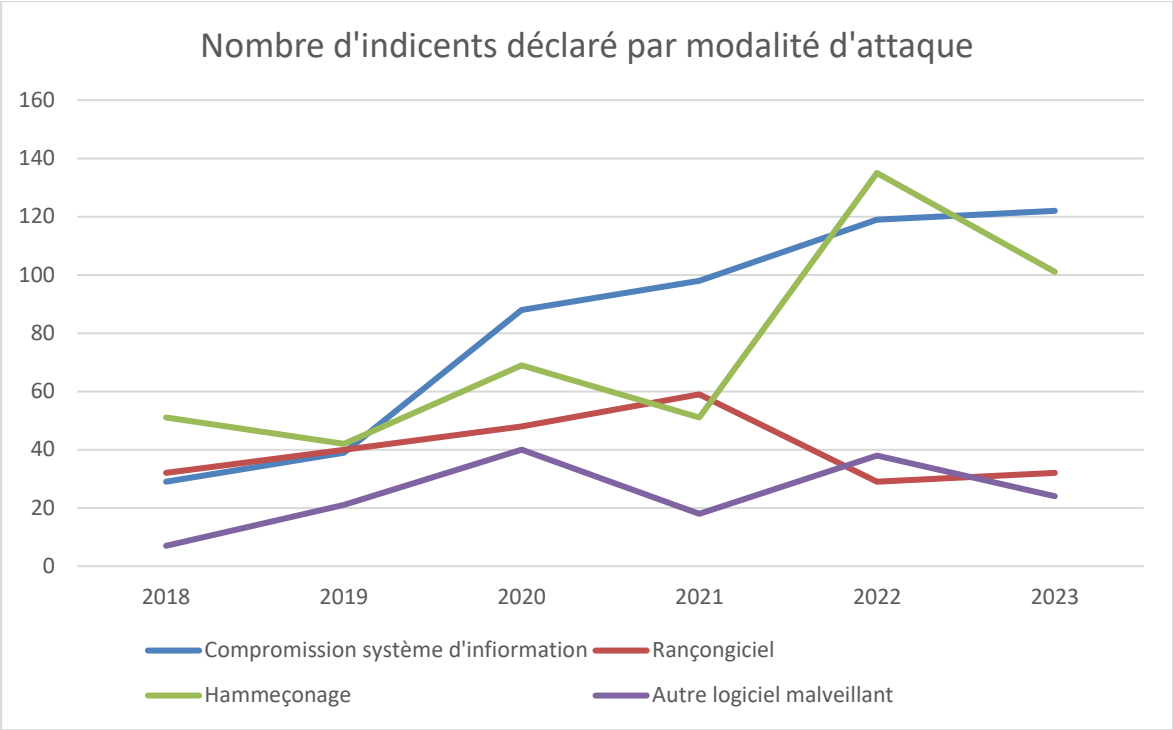

Figure 2 – Evolution du nombre de signalement d'incidents numériques assimilables à des cyberattaques (la plupart sont déjouées à temps, avec un impact inférieur à quelques jours) – Source : données compilées issues des rapports 2018 à 2023 de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé

On observe néanmoins un accroissement des signalements, du nombre d'incidents pris en charge par l'ANSSI, a fortiori de grande ampleur, mais aussi une spécialisation des attaques. En effet, la doctrine de l'Etat français, qui s'impose aux établissements publics de santé, est de ne pas payer les sommes demandées lors d'attaques par rançongiciel, qui visent donc désormais surtout les prestataires de services utilisés par les hôpitaux et non les hôpitaux eux-mêmes. On observe parallèlement une augmentation de la part des compromissions des systèmes d'information visant à en dérober les données, forme d'attaque plus ciblée, qui nécessite de bien connaître la cible avant l'attaque.

Cette mutation des attaques est aussi à corréler à une montée en gamme des cyberdéfenses des hôpitaux, dictée par un ensemble de texte.

1.1.2 D'une simple sécurisation des données à une sécurisation du système d'information

La construction des défenses numériques de hôpitaux s'est d'abord faite dans une logique de sécurisation et de fiabilisation du système d'information et dans une moindre mesure pour parer la fuite de données de santé ou personnelles.

Cette logique s'illustre notamment dans la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), mise en place dès 2013 afin d'encadrer les règles de sécurité pour la santé numérique. Elle constitue un premier canevas concernant les niveaux de protection attendu des données dans le milieu de la santé, sans concerner spécifiquement les hôpitaux. Elle vise surtout à mettre à niveau les SI des hôpitaux, toujours en construction, et à faire respecter les normes déjà en place sur l'hébergement des données médicales et personnelles par exemple.

Le « Guide pour les directeurs d'établissement de santé - Introduction à la sécurité des systèmes d'information », publié en 2013 par la DGOS, et qui fait partie de la PGSSI-S illustre ces premiers pas dans la sécurisation du SI, en exposant des cas réels qui se sont produits du fait de manquement à certaines obligations : « Suite à des raisons historiques dans un établissement, un pont de visioconférence été ouvert sur Internet en clair. Les visioconférences qui servaient à des conversations d'ordre médical, étaient accessibles à tout le monde depuis Internet » « A cause de cette ignorance du risque, des données médicales se sont retrouvées indexées sur les moteurs de recherche internet début 2013 dans un hôpital ».

Cependant, bien que ce défaut de sécurité et de fiabilité des SI des hôpitaux était connu des ministères de tutelle, il ne faisait pas partie des objectifs principaux du programme « Hôpital numérique » portant sur la période 2012-2016. Seul un des trois objectifs mentionne cet aspect sécurité : « Amener l'ensemble des établissements de santé à un niveau de maturité de leurs systèmes d'information suffisant pour améliorer significativement la qualité, la sécurité des soins et la performance dans des domaines fonctionnels prioritaires, sur un socle assurant la sécurité des données ». Concrètement, les ambitions du programme se limitaient à l'homologation des logiciels utilisés, sans contrainte supplémentaire sur le SI de l'établissement.

Le plan d'action sur la sécurité des systèmes d'information (dit « Plan d'action SSI ») viendra pallier ce manque en 2016, en visant spécifiquement à améliorer la sécurité des SI des hôpitaux, le « Plan d'action SSI ». Ce plan visait à la mise en œuvre de mesure prioritaire, à mettre en œuvre sous 6, 12 ou 18 mois, afin d' « opérer une mise à niveau minimale de la sécurité des systèmes d'information ». Le caractère minimal de ce plan est à souligner, ce plan ne visant pas à améliorer la sécurité des SI les plus robustes comme l'illustre certain de ces objectifs opérationnels : mise en place d'antivirus et de pare-feu, mise à jour des système d'exploitation, sécurisation des comptes utilisateurs par mot de passe, différenciation des comptes utilisateurs en fonction de leur profil (simple utilisateur,

utilisateur accrédité, administrateur), mise en place de mot de passe pour accéder aux réseaux de l'établissement,…

Ce retard dans la sécurisation des SI des hôpitaux a manifestement empêché de traiter un sujet pourtant maintes fois évoqué dans ces guides, celui de la résilience des établissements de santé face aux cyberattaques. Le sujet est pris plus frontalement à partir de 2017, avec la rédaction du « Mémento DGOS à l'usage du directeur d'établissement de santé, connaître vos risques pour mieux y faire face » en 2017, qui prend pour exemple la première cyberattaque d'ampleur sur un hôpital, le *Presbyterian Medical Center* à Los Angeles. Cependant l'accent est mis principalement sur la protection des données, à l'aune du futur RGPD (mis en place le 25 mai 2018) et de la mise en place d'une certification pour les hébergeurs de données de santé, ainsi que sur le respect des droits des usagers vis-à-vis de leurs données (CNIL). La résilience face aux cyberattaques, mais surtout le maintien de l'activité une fois la crise survenue n'est abordée que très marginalement, en reprenant néanmoins les outils centraux de ce sujet tels que l'illustre l'encart ci-contre.

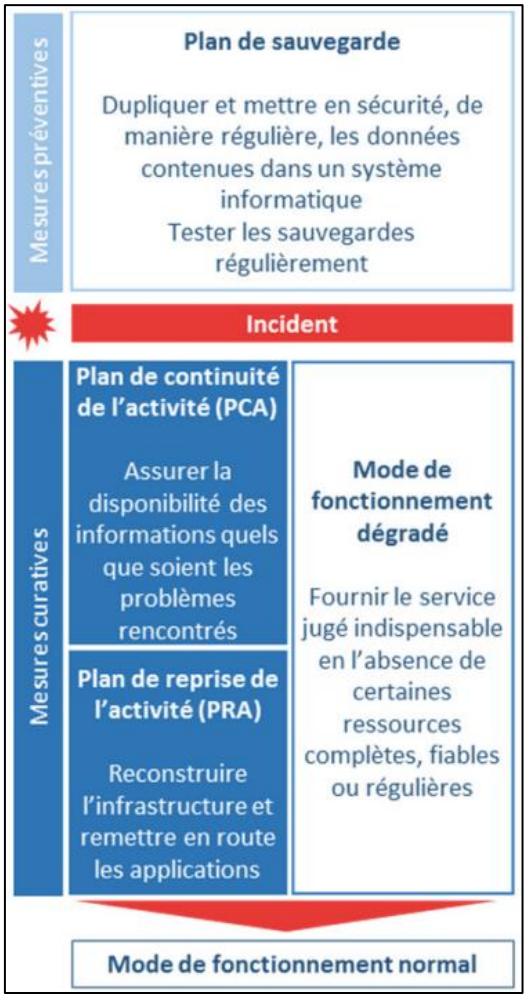

Figure 3 – Extrait du Mémento DGOS « connaître vos risques pour mieux y faire face », 2017

1.1.3 Malgré des plans de mise à niveau des défenses des hôpitaux, la résilience des hôpitaux face aux cyberattaque reste largement impensée jusqu'au début des années 2020

Il est à noter que dans d'autres champs, y compris publics, la menace cyber est prise très au sérieux dès les années 2010 voire 2000.

A titre d'exemple il est intéressant de noter l'existence du « Guide pour réaliser un plan de continuité d'activité » rédigé par le Secrétariat général de la défense et de la sécurité nationale en 2013. Ce guide, qui n'a pas vocation à irriguer spécifiquement des réflexions

issues du monde de la santé, reste d'une actualité frapante et y expose ainsi le rôle d'un plan de continuité d'activité (PCA) : « Le PCA décrit la stratégie de continuité adoptée pour faire face, par ordre de priorité, à des risques identifiés et sériés selon la gravité de leurs effets et leur plausibilité. Il décline cette stratégie en termes de ressources et de procédures documentées qui vont servir de références pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini, lorsque celui-ci a été interrompu à la suite d'une perturbation importante ».

En un sens, cette définition n'est donc pas très éloignée de celle du Plan blanc selon la définition du ministère de la santé : « Chaque établissement de santé est doté d'un dispositif de crise, dénommé plan blanc d'établissement, qui lui permet de mobiliser immédiatement les moyens de toute nature dont il dispose en cas d'afflux de patients, ou pour faire face à une situation sanitaire exceptionnelle. Les étapes de mobilisation des moyens humains et matériels sont déclinées de façon graduée et sectorielle ».

De la même manière, un volet numérique du plan blanc doit répondre aux mêmes exigences et proposer également des étapes de mobilisation des ressources et procédures adaptées. Plan blanc numérique et plan de continuité d'activité en cas de cyberattaque sont, sinon équivalents, du moins très proches en termes de contenu et de construction.

Le Guide d'aide à la préparation au volet numérique du Plan blanc publié en 2023 par la DGOS « vise à fournir un cadre méthodologique et pratique pour prévenir le risque numérique et adopter une conduite collective visant à gérer et sortir au mieux d'une crise numérique ». La lettre d'information qui accompagne la publication de ce guide précise que la naissance de ce guide est consécutive à l'augmentation du nombre de cyberattaques de 2019 à 2021.

Pourtant le guide fait le choix d'aborder la continuité de l'activité uniquement par le prisme de la continuité informatique, les plans de continuité et plan de reprise mentionnés ne concernant que ceux du système d'information. Or le principe d'une cyberattaque est de ne plus pouvoir compter sur le système d'information, et un plan de continuité doit permettre aux services la poursuite de leur activité en l'absence de celui-ci. Afin de pouvoir parer à toute éventualité – concrètement à tous les scénarios de cyberattaque possibles – il faudrait donc mettre en place un SI redondant, de manière à assurer la continuité de chacune des fonctionnalités du SI qui serait perturbé lors d'une cyberattaque. Cependant la nature imprévisible des cyberattaques empêche de connaître à l'avance les fonctionnalités qui seront perturbées en raison de la cyberattaque ou des conséquences de l'endiguement de celle-ci (fréquemment, le réseau informatique d'un établissement attaqué est

volontairement coupé par l'établissement lui-même afin d'endiguer la propagation de la cyberattaque, emportant avec lui la plupart des fonctionnalités du SI).

Ainsi plutôt que de miser sur une reprise rapide du système d'information (il est utile de rappeler ici que les hôpitaux de Versailles et du Sud francilien, victimes d'importantes cyberattaque ne sont toujours pas pleinement remis plus d'un an et demi après), il convient donc surtout de préparer la continuité des services de soins en l'absence de SI ou avec un SI fortement réduit. Ce sujet est abordé dans la troisième partie de ce guide, qui traite de l'organisation des soins.

Dans le guide, il n'est pas question d'y faire face, ce dernier se bornant à lister les impacts potentiels sur l'hôpital en cas de cyberattaques : risque de perte de la téléphonie, des planning de blocs opératoires, incapacité à réaliser des admissions, impossibilité d'assurer la prise en charge des patients dont l'état clinique est critique, dégradation de la qualité et de la sécurité de soins, perte de la connexion aux dispositifs médicaux, perturbation des fonctions logistique et techniques, interruption des fonctions administratives, etc.

Concernant la continuité des soins le guide ne préconise aucune méthodologie particulière et dresse simplement le constat suivant : « Chaque service de soins qui utilise des applications logicielles « métier » critiques doit pouvoir continuer à travailler en l'absence de ces applications. En pratique, chaque service devra s'approprier les procédures dégradées définies par l'établissement, s'assurer de leurs mises à jour et les adapter, le cas échéant, à leurs modalités spécifiques de fonctionnement ».

La solution décrite dans ce guide pour faire face à une cyberattaque revient essentiellement à se délester d'un maximum d'activité, par le transfert de patient vers les établissements du territoire et la déprogrammation, piloté par l'ARS.

Si cette solution est réalisable pour de petit centre hospitalier, elle ne l'est pas pour des centres hospitaliers de taille importante et/ou dont l'offre de soins n'est pas substituable sur le territoire, et devient aberrante dans le cas des CHU les plus importants et les activités les plus pointues qui ne sont exercées que par quelques établissements à une échelle suprarégionale, voire nationale. C'est particulièrement vrai pour les HCL, l'AP-HM et l'AP-HP, qui occupent des positions quasi-monopolistiques sur l'offre de soins hospitalière de leur territoire (75% des lits MCO de la région Île de France sont situés dans des sites de l'AP-HP), et dont l'interconnexion des systèmes d'information fait présager une chute de l'établissement entier en cas d'attaque réussie sur l'un des sites.

1.1.4 Face à un risque de cyberattaque protéiforme les guides nationaux peinent à établir une méthodologie de construction des plans de continuité d'activité

Avec la version 2024 de la certification des établissements de santé par la HAS, dont le critère 3.6-02 stipule que « les risques de sécurité numérique sont maîtrisés », et surtout face à l'essor des cyberattaques de plus en plus importantes, la rédaction de plans de continuité d'activité (PCA) opérationnels devient, sinon une obligation réglementaire, du moins un sujet de première importance. Le critère de certification reste néanmoins vague sur les attentes précises de ce plan, avec pour la gouvernance : « L'établissement a déployé un plan de continuité d'activité et un plan de reprise d'activité dans tous les secteurs », et pour les professionnels : « Les équipes savent mettre en œuvre à tout moment leur plan de continuité d'activité et leur plan de reprise d'activité ».

Cependant, aucune méthodologie détaillée pour la construction de PCA opérationnels dans chacun des secteurs d'un hôpital, visant à maintenir un haut niveau d'activité, de sécurité et de qualité des soins (et l'on pourrait ajouter sans compter sur le délestage et la déprogrammation comme moyens principaux de résilience), ne semblait être proposée par les organismes de tutelle jusqu'en 2023.

L'obligation de réaliser des exercices cyber dans les établissements de santé avant fin 2023, puis une fois par an, annoncée par une note d'information à destination des directions générales des ARS le 14 décembre 2021, ainsi que la naissance du plan CaRE (Cybersécurité Accélération et Résilience des Établissements) pour la période 2023-2027, ont néanmoins mis l'accent sur la nécessité pour chaque établissement de se doter de PCA. Contrairement aux quelques jours d'indisponibilité des systèmes d'information (SI) observés avant 2020 dans les établissements cyberattaqués, le plan CaRE concède désormais que « suite aux attaques, la plupart des établissements sont contraints de travailler durant de longs mois pour retrouver leur niveau d'activité d'avant-crise ».

Cette prise de conscience tardive a mené à la création de kits d'exercice de crise cybersécurité, destinés à permettre aux établissements de réaliser de tels exercices en autonomie. Ces premiers exercices ont également révélé à certains établissements leur insuffisante résilience face à une cyberattaque, les incitant à demander un accompagnement à la rédaction de PCA de la part du programme CaRE : « les établissements sanitaires et leurs représentants ont exprimé le besoin d'être accompagnés dans la formalisation et la mise en œuvre de leur Plan de Continuité d'Activité (PCA) et de leur Plan de Reprise d'Activité (PRA) ».

En réponse, l'ANS a produit des kits PCA-PRA visant à autonomiser les établissements dans la construction de leurs PCA. Ces kits restent néanmoins peu opérationnels et ne détaillent pas les processus permettant de trouver des solutions de continuité d'activité, qui sont le cœur des PCA, car ce sont elles qui permettent, en définitive, la continuité des activités hospitalières. Ils fournissent toutefois un cadre « stratégique » pour la conduite de ce projet, en recommandant les personnes à associer.

La difficulté de fournir une méthodologie précise repose essentiellement sur le caractère imprévisible des cyberattaques, dont les conséquences sont difficilement anticipables : simple perte des emails, perte de certains serveurs, ciblage de quelques applications critiques (dossier patient, système de gestion des commandes, système de gestion des médicaments), perte du réseau, ou une combinaison de ces facteurs. Le périmètre et l'ampleur d'une potentielle cyberattaque étant incertains, il devient difficile de proposer un plan capable de prendre en compte l'ensemble des scénarios probables. La diversité des attaques subies par les établissements touchés rend également complexe l'évaluation du scénario le plus probable, lequel dépend non seulement de la nature de l'attaque mais aussi de la configuration du SI, propre à chaque établissement.

Il revient donc, pour le moment, à chaque établissement de s'emparer de ce sujet et de se préparer en fonction de ses caractéristiques propres, qui sont, dans les détails, uniques.

Il convient néanmoins de noter la très récente création des centres régionaux de ressources cybersécurité (CRRC). D'après la note d'instruction N° DNS/2024/54 du 2 juillet 2024 relative aux missions des centres régionaux de ressources cybersécurité (CRRC) et à leur financement, le CRRC « met à disposition des établissements de la région une offre organisationnelle et technique de services dédiée au renforcement de la cybersécurité des établissements : celle-ci doit répondre à des besoins identifiés comme prioritaires ». Les missions précises confiées aux CRRC restent à la discrétion des ARS, en fonction des priorités locales, et pourront inclure, à titre d'exemple, « l'accompagnement des ES et ESMS dans le déploiement du Plan de Continuité et de Reprise d'Activité (PCRA) "CaRE" » ou encore la « construction d'un dispositif régional permettant de faire face à un incident cyber ». Au vu de leur faible niveau de financement, les capacités des CRRC risquent néanmoins d'être limitées, avec un budget total de 18 millions d'euros pour le secteur sanitaire, réparti sur 2831 établissements de santé.

2 Si le besoin de construire des PCA est désormais reconnu, une méthodologie unie de construction reste à définir et est ici proposée

2.1.1 Quelle approche utiliser et quel scénario retenir

Dans un premier temps, le sujet sera nécessairement abordé par le haut, puisque la continuité des opérations d'un établissement incombe au directeur d'hôpital. Il s'agit en cela de l'orientation naturelle du projet. De plus, c'est également l'orientation donnée par les pouvoirs publics, les autorités de tutelle, et les organisations qui traitent du sujet pour le secteur sanitaire, ce qui correspond aussi à la vision de la certification version 2024.

Dès lors, il peut être tentant d'adopter une approche descendante, mais cela revient à oublier que le but fondamental des PCA est le maintien des activités opérationnelles de l'établissement, lesquelles se déroulent sur le terrain, au sein des services.

Il ne faut certes pas négliger les travaux et préparations nécessaires pour structurer ou adapter le fonctionnement d'une cellule de crise à la gestion particulière d'une cyberattaque, mais tous les éléments en question sont entre les mains de la direction et sont a priori aisément mobilisables. De plus, en contexte de crise, la cellule de crise dialoguera essentiellement avec des organisations non touchées par la cyberattaque et ayant maintenu leurs capacités opérationnelles (ARS, ANSSI, etc.).

De la même manière, le pilotage par le haut reste une approche cohérente dans la préparation préalable de la DSI, en lien avec les sujets évoqués en première partie (cartographie du SI, de ses ressources, de ses logiciels, renforcement des défenses), mais également dans les sujets de coopération et de mutualisation territoriales (CERT, CRRC, GRADeS, etc.).

Il en va de même pour les éventuels efforts de collaboration ou de contractualisation avec des organismes capables de permettre la substitution des activités des plateaux techniques, qui, étant très fortement informatisés, sont logiquement les plus complexes à préparer.

Une approche descendante rencontre néanmoins rapidement des limites. Bien qu'un hôpital soit une structure particulièrement hiérarchisée et verticale, il repose concrètement sur des activités pouvant être indépendantes et sur des unités relativement autonomes, au moins sur leur cœur de métier. De plus, ces unités sont épaulées par tout un arsenal de fonctions supports, mais elles témoignent aussi de relations d'interdépendance, ce qui

complexifie une approche purement descendante, voire ascendante. Ces interconnexions et interdépendances entre les secteurs cœur de métier (services de soins, plateaux techniques ou médico-techniques) et les ressources (SI, fournitures logistiques, gestion du matériel, équipement biomédical, accès au réseau et connectivité des appareils, etc.) plaident également pour une approche plus décentralisée.

En réalité, le management procédural devra être adapté en fonction des besoins et des actions à mettre en œuvre. Trois niveaux sont ainsi à distinguer :

- Pilotage stratégique : ouverture de l'établissement sur l'extérieur/territoire, relations partenariales, prise de décisions stratégiques concernant les éventuels investissements à faire, cadrage de la démarche (quel scénario, quelle temporalité, quels moyens, quel niveau d'exigence, quelles ressources humaines pour mener à bien ce projet), définition du périmètre et d'un calendrier. Ce niveau est celui du comité stratégique et/ou de pilotage, et ses productions seront consignées dans ce qui est fréquemment désigné comme le PCA cadre.
- Niveau intermédiaire : agrégateurs d'informations et recensement des besoins opérationnels. Les services ayant un certain niveau d'indépendance mais s'appuyant sur des fonctions supports communes, il est nécessaire d'envisager un niveau commun capable de centraliser les échanges et de dialoguer directement avec ces fonctions techniques et/ou administratives. Ce niveau est aussi le premier niveau de cohérence permettant de mutualiser et de mettre en commun les besoins ainsi que les solutions trouvées pour un service particulier.
- Niveau opérationnel : Il constitue le niveau du travail de fond et concerne aussi bien les services que les fonctions supports. Il s'agit du niveau chargé de la recherche de solutions techniques, de la rédaction de guides ou de procédures, et de la création de processus permettant de fonctionner en mode dégradé sur le long terme.

L'interconnexion et les relations d'interdépendance, ainsi que l'acquisition de nouvelles connaissances ou la création de nouvelles solutions à mesure que le projet avance, risquent de rendre nécessaires des allers-retours entre ces différents niveaux, mais aussi entre les étapes présupposées du processus. L'émergence de nouveaux besoins, de scénarios non préalablement identifiés, et le croisement d'informations sont autant de développements qui peuvent nécessiter un retour en arrière sur le projet.

La nature disséminée de l'information, partagée entre des secteurs ou domaines pas nécessairement en relation étroite, aboutira à une connaissance imparfaite de la situation,

poussant à des hypothèses de travail plus ou moins robustes, qui ne s'éclairciront qu'au fur et à mesure de l'avancement du projet.

Ainsi, la conduite de ce genre de projet est tout sauf linéaire, car il s'agit, au fond, de toucher à l'ensemble des processus qui animent un hôpital, leur basculement en mode dégradé risquant souvent d'impacter le fonctionnement d'autres processus, qui ne seraient pourtant pas touchés en eux-mêmes.

La conduite du projet en elle-même est donc un processus complexe, non linéaire, qui repose sur des hypothèses de travail imparfaites. Afin de se doter d'un plan robuste capable de fournir des réponses utiles en toute circonstance, il convient donc de ne pas s'éparpiller en de multiples scénarios de cyberattaque, obligeant à autant de plans que de types d'attaques possibles. Il n'existe en effet pas de cyberattaque type, et l'approche la plus pertinente revient donc à se préparer au pire, avec un scénario le plus large possible. Ce scénario catastrophe retiendra la perte de l'ensemble des moyens assimilés au SI pendant une durée de trois mois.

Ce délai est indicatif, et repose sur l'utilisation d'ordres de grandeur pour proposer une temporalité générique des conséquences d'une cyberattaque : trois heures pour prendre conscience de la crise, trois jours pour mesurer l'ampleur de l'attaque et de ses conséquences, trois semaines pour débuter un fonctionnement dégradé de routine et la reprise de certaines activités, trois mois pour commencer la reconstruction d'un SI primitif, trois ans pour un complet retour à la normale. Cette temporalité empirique est effectivement observée dans les établissements subissant des cyberattaques majeures ; ainsi, les centres hospitaliers de Versailles et du Sud francilien, attaqués il y a un an et demi et deux ans, ne sont toujours pas pleinement remis de la crise.

2.1.2 Bâtir un socle solide de fonctionnalités préservées en cas de cyberattaque totale

Puisque le scénario le plus fiable est celui d'une cyberattaque totale, la suite logique est de déterminer les éléments dont la fonctionnalité ne sera pas perturbée ou sera perturbée de manière minimale, afin de construire un socle des éléments préservés en cas de cyberattaque. Ce socle servira à la construction des premiers PCA, de type « médecine de guerre », dont le but sera de surmonter la phase la plus aiguë de la crise (de sa survenue à J0 jusqu'à J+3 semaines).

Forts de cette première expérience, des connaissances acquises, des dispositifs construits, des informations et soutiens obtenus de la part des structures de tutelle ou pouvant apporter

leur aide ou expertise (ANS, ANSSI, ARS, CERT, Grades, CRRC, etc.), il sera alors possible de construire des scénarios plus fins et d'y apporter une réponse plus précise. La mise en place de certaines organisations et solutions de continuité dans le cadre des premiers PCA (par exemple, l'assurance de la disponibilité de la biologie sur tout ou partie des examens) permettra de bâtir des PCA capables de reprendre ces acquis et d'explorer des hypothèses de cyberattaques plus diverses et précises.

Ainsi, si la réalisation des PCA conduit à la mise en place d'un système permettant de disposer rapidement de postes informatiques sains en cas de cyberattaque, cela sera à prendre en compte dans l'actualisation ou la réalisation de nouveaux PCA pour d'autres services, par exemple.

Pour le moment, revenons à notre hypothèse minimale et de travail, celle d'une indisponibilité totale du SI. Cela revient à considérer que les postes informatiques, l'accès au réseau et aux données de l'établissement, et plus généralement tout élément connecté au SI, sont indisponibles suite à une cyberattaque. Les impacts seront plus ou moins larges au cas par cas, en fonction des dispositions précises qui existent au sein de chaque établissement, et il conviendra donc d'étudier l'impact d'un tel scénario sur un large périmètre. Peuvent ainsi également être concernés le réseau téléphonique (particulièrement pour les bâtiments récents, suite à l'arrêt des lignes téléphoniques physiques prévu pour 2030, qui passent désormais par le réseau de l'établissement), les systèmes de GTC/GTB, les moyens d'impression, les contrôles d'accès, etc.

La réalisation d'un bilan par les services techniques et la DSI doit donc être la plus exhaustive possible et produire un résultat lisible afin que chacun puisse s'en approprier les résultats, les services en particulier.

À l'inverse, il faut également dresser une liste des fonctionnalités qui ne seront pas perturbées, afin de s'assurer qu'une vérification a été faite en ce sens, sans oublier que certaines des ressources consommées par l'hôpital ne sont pas produites en son sein : eau, électricité, réseau de télécommunications mobiles, etc. Cela peut également être le cas de certains processus informatiques, qui ne dépendent pas directement de l'hôpital et qui pourront rester accessibles même si les serveurs de l'établissement ne sont plus fonctionnels. C'est le cas de processus proposés par des prestataires, hébergés sur leur propre matériel et auxquels les agents de l'établissement accèdent par une simple connexion internet.

2.1.3 La recherche d'une exhaustivité ne doit pas faire obstacle au lancement du processus de conception des PCA qui est facilité par la sélection de services pilotes

La constitution d'un socle de processus ou de fonctionnalités génériques qui fonctionneront en cas de cyberattaque totale doit rechercher l'exhaustivité, sans nuire au démarrage du projet auprès des services. Cela permettra d'anticiper et de répondre à un certain nombre de questions générales qui seront invariablement posées au niveau des services (« la ventilation du bloc opératoire marchera-t-elle ? », « les contrôles d'accès seront-ils maintenus ouverts ou fermés ? », etc.), mais certaines resteront en suspens car dépendant d'autres services ou non anticipées (« les pousse-seringues ont-ils besoin du réseau pour fonctionner ou sont-ils autonomes ? Quelles fonctionnalités sont perdues ? »).

Une approche possible est de poursuivre la cartographie plus avant, en explorant ces questions spécifiques avant la rencontre avec les services. Néanmoins, dans un souci de rationalisation du temps et des ressources à affecter au projet de création de PCA, l'approche de ces questions précises par les services semble être la plus pertinente. Elle permet également de donner du concret au processus, en posant des questions précises aux personnes chargées de ces sujets techniques plutôt que de rester dans un point de vue théorique et purement technique.

Par ailleurs, il ne faut pas sous-estimer les ressources internes et les connaissances que peuvent avoir les services sur leurs fonctions supports, et il se peut qu'une grande partie des réponses recherchées vienne par ce biais. Cette approche permet également de confirmer ou d'infirmer des hypothèses initiales de travail sur la criticité réelle de tel ou tel service. Il n'est pas nécessairement aisé de quantifier a priori d'un point de vue extérieur le degré d'indépendance potentiel d'un service vis-à-vis du SI, ni le degré de dépendance à d'autres services qui auraient pu, à première vue, être jugés moins critiques.

Cette démarche d'approche rapide du problème par le prisme des services permet également d'identifier ceux qui seront les plus moteurs, et ceux qui seront davantage suiveurs. L'ampleur du sujet et le caractère très novateur de la démarche (se passer d'informatique), qui va à l'encontre de ce qui s'est fait ces dernières décennies, peut rendre complexe le lancement de la démarche, peut-être moins pour le comité de pilotage que pour les effecteurs intermédiaires ou encore les services. Cela permet enfin de personnaliser la démarche et d'identifier les services qui seront les plus indépendants et ceux qui auront le plus besoin d'aide.

Puisque le but est de maintenir la continuité opérationnelle, métier et de terrain, ce travail pourrait et devrait presque être uniquement mené par les services. Cependant, au vu des éléments évoqués ci-dessus, mais aussi dans un souci de cohérence vis-à-vis de la stratégie globale et de rationalisation des moyens (mettre en commun les besoins et solutions qui sont partagés), il convient de superviser, voire d'organiser ce processus par un niveau intermédiaire commun aux différents services.

L'adoption de cette organisation permet également de ne pas s'éloigner du cadre de la démarche, qui vise d'abord à identifier les besoins, puis à proposer des solutions de continuité pour faire face en cas de cyberattaque. Sans cela, le réflexe peut rapidement être de catégoriser la tâche comme impossible, ou alors de proposer la mise en place de processus informatiques en boucle fermée afin de préserver les capacités informatiques, particulièrement dans les secteurs très informatisés. Cette possibilité n'est pas réaliste financièrement (cela reviendrait à démutualiser les moyens informatiques physiques et numériques de chaque service demandeur), ni structurellement, la fonctionnalité d'un SI hospitalier reposant sur la circulation de l'information d'un service à l'autre. Au contraire, certains services pourront avoir des facilités à revenir vers des processus non informatisés, notamment en raison de dématérialisations récentes ou encore inachevées (avec des dossiers patients encore en format papier).

Concernant le sujet de l'embarquement des personnes sur le thème de la préparation aux cyberattaques, de nombreux interlocuteurs ou services peuvent considérer qu'il s'agit d'un sujet stratégique et relevant de la DSI, qui ne les concerne pas. Ils peuvent également témoigner d'un sentiment de sidération et se sentir dépassés face à un sujet d'une envergure trop importante et complexe pour être abordé. Dans les deux cas, une première réunion de sensibilisation visant à exposer le scénario retenu (cyberattaque totale), les premiers éléments de certitudes (ce qui risque de ne plus fonctionner, ce qui fonctionnera en toute situation), mais surtout à faire comprendre que ce n'est pas un sujet qui peut être traité par la DSI, car il implique essentiellement les processus métiers des services eux-mêmes. Ces sentiments d'être dépassé et de peur, loin d'être des freins, peuvent également être des moteurs, faisant tomber les freins et barrières éventuelles à l'implication des acteurs dans le projet, mais il faut alors avoir un socle tout aussi solide sur lequel construire. D'où l'intérêt d'établir une cartographie robuste des fonctions et processus qui ne seront pas impactés en cas de cyberattaque, évoquée précédemment.

2.1.4 Le rôle des effecteurs intermédiaire, entre stratégie et opérationnel

Entre le pilotage stratégique, l'expression des besoins et la recherche de solutions qui peuvent avoir lieu sur le terrain, il est nécessaire de constituer une structure intermédiaire capable d'éclairer ces solutions, de fournir des réponses à des questions techniques, de proposer des solutions nouvelles, et d'évaluer la possibilité de changements organisationnels ou techniques (possibilité de mettre hors réseau certains équipements, possibilité d'acquérir des modules, logiciels, etc., permettant de faire tourner certains processus informatiques même en cas de cyberattaque totale sur l'établissement). Concrètement, cette structure agit comme un concentrateur d'informations et un interlocuteur entre les différents acteurs stratégiques, de support (techniques, informatiques, logistiques) et les services opérationnels.

Ce rôle nécessite à la fois une bonne connaissance des métiers de l'hôpital, des services, des directions et fonctions supports, ainsi qu'une capacité à convaincre les services de s'engager. Le besoin de concentrer les informations en un point unique, de bénéficier pour toutes les parties prenantes d'un interlocuteur unique, et le développement d'une expertise reconnue plaident en faveur de la désignation d'un responsable unique ou d'un nombre très restreint de personnes.

Cependant, l'ampleur de la tâche et le besoin d'avancer rapidement sur ce sujet peuvent justifier de ne pas confier cette responsabilité à une seule personne. De plus, le caractère innovant de ce genre de projet nécessite une intelligence collective et un partage de points de vue. L'adoption d'une petite équipe permettrait aussi une répartition des rôles ou l'usage des personnes comme relais dans des domaines techniques, en intégrant par exemple des individus issus des directions techniques et SI, ou encore de la qualité.

Bien que des prestataires existent pour proposer un appui, voire le sous-traitement de ce processus, la nouveauté de ce type de projet dans le domaine hospitalier, très complexe mais éloigné des domaines ayant développé des plans de continuité (domaine industriel ou de la défense), ne permet pas à ces prestataires de fournir une aide adaptée. Cette compétence va probablement se développer dans les années à venir, avec le déploiement croissant du sujet de la cyber-résilience des hôpitaux et l'obligation de mettre en place des PCA. Pour l'heure, bien que ces prestations existent, elles n'ont pas su satisfaire les hôpitaux clients, les compétences de ces entreprises se limitant à la réalisation de BIA.

De plus, confier cette mission à une structure externe à l'hôpital empêche le développement d'une expertise en interne, alors même que les PCA ont vocation à évoluer avec les

menaces liées aux cyberattaques, les mutations du SI, et les évolutions au sein des services et de l'établissement en général. À plus court terme, il n'est pas garanti que le recours à une prestation de conseil soit plus efficace financièrement, en raison également de la légitimité partielle auprès des professionnels, d'une connaissance partielle des métiers de l'établissement, et du risque de provoquer un désengagement des professionnels qui sont pourtant les plus à même de produire les solutions recherchées.

Être intégré à l'hôpital et bénéficier d'une connaissance de celui-ci autrement qu'à travers ce seul projet est donc un élément crucial pour la réussite de la construction des PCA, mais aussi pour tirer le meilleur des parties prenantes en leur témoignant la pleine participation de ces acteurs intermédiaires, qui ont tout autant qu'eux intérêt à voir ce projet réussir.

Plus généralement, il convient de souligner que les professionnels eux-mêmes peuvent, par leurs expériences, avoir engrangé de nombreuses connaissances sur le fonctionnement technique de l'hôpital. Ces connaissances sont disséminées dans l'ensemble de l'établissement : dans les services techniques, logistiques, informatiques, mais aussi de soins et médico-techniques, et constituent des atouts précieux.

Mon expérience me pousse à formuler la recommandation suivante : la démarche de construction des PCA nécessite des acteurs très intégrés, aussi bien dans le milieu hospitalier que dans la démarche elle-même, et il convient donc de proscrire l'usage d'acteurs externes, sauf en cas d'absolue nécessité pour les premières étapes du projet. Cela se ferait au détriment de la perte de tous les avantages de réaliser cette démarche en interne : structurer une réflexion adaptée, acquérir une expertise locale, déléguer des compétences aux acteurs de terrain, diffuser le sujet cyber voire créer une culture cyber. Enfin, cela créerait un risque, en cas d'insatisfaction de la prestation, de laisser une mauvaise impression des sujets cyber auprès des acteurs de terrain.

2.1.5 Le BIA un outil crucial aux premières phases de la construction de PCA

Les bilans d'impact d'activités sont des outils pratiques visant à permettre de lister les impacts potentiels d'une cyberattaque sur les activités d'un service. Au-delà de ce simple catalogue, le but est de comprendre l'ensemble des activités du service, sur l'ensemble des patients. Ils permettent de prendre la mesure de tous les processus à l'œuvre, des outils et équipements utilisés, mais aussi de lister les éventuelles procédures dégradées et l'aide qu'elles peuvent apporter.

De la même manière que le socle de fonctionnalités et équipements disponibles à l'échelle de l'établissement en cas de cyberattaque, cette liste doit viser une forme d'exhaustivité. Elle permet à son tour de constituer une base solide sur laquelle baser le PCA, à l'échelle du service, mais également de déceler les potentiels facteurs d'aggravation de la crise (heure, moment de la semaine, de l'année où une cyberattaque pourrait déstabiliser plus facilement un service). Ce processus est très chronophage (estimé à plusieurs jours dans les kits de l'ANS), mais il doit être exhaustif pour permettre une pleine continuité des activités du service, de l'entrée à la sortie du patient. Pour un service de soins, il s'agira par exemple : des modalités de prise de rendez-vous, des plannings d'entrée dans le service, des circuits de brancardage, de la disponibilité des informations du patient et de son dossier, du système d'identitovigilance, du système de prescription, des équipements de (télé-)surveillance de l'état clinique du patient, de la prise de repas, des équipements, examens ou machines susceptibles d'être mobilisés dans le soin du patient, de la récupération des résultats d'examens (interne ou externe), des circuits logistiques susceptibles d'être mobilisés dans le soin du patient (médicaments, produits sanguins, DMI, fournitures hôtelières, etc.), du système de communication au sein de l'équipe soignante et au sein de l'équipe médicale, des modalités de réalisation des transmissions, des modalités de tenue des staffs, des modalités de sortie du patient, des modalités de rédaction de comptes rendus, du transfert de patients vers d'autres établissements…

En raison des activités très différentes que peuvent réaliser un service de médecine, de chirurgie, un plateau médico-technique, une unité de soins de longue durée, ou un service technique, il convient d'adapter une éventuelle trame en fonction des besoins. Ainsi, les BIA, plus qu'une trame physique, doivent surtout être un moyen d'engager une discussion de fond sur l'ensemble des activités d'un service particulier.

Le caractère exhaustif de la démarche implique de ne pas avoir un interlocuteur unique côté service, mais des professionnels de différents métiers, présents sur le terrain. Le chef de service n'est ainsi pas nécessairement au courant de l'ensemble des détails techniques de l'organisation d'un service ou peut avoir une vision trop macroscopique. De même, le cadre de santé n'est pas forcément au courant de l'organisation précise ou de l'ensemble des activités des paramédicaux.

En plus de dresser un panorama de l'ensemble des activités et de leur degré de dépendance à l'informatique (besoin de tel logiciel, de tel poste informatique, du réseau, systèmes de sauvegarde ou redondances non numériques existantes), le BIA s'attachera aussi à prioriser chacune des activités en précisant pendant combien de temps ces activités peuvent être maintenues même en l'absence de tout SI. Ces durées risquent dans un

premier temps d'être très courtes (ne dépassant pas les 12h) et corrélées aux durées maximales pendant lesquelles les procédures dégradées peuvent être maintenues.

Néanmoins, les éventuelles procédures de mode dégradé existantes risquent d'être relativement incomplètes ou de se reposer sur le dysfonctionnement d'un élément précis du SI, en présupposant le bon fonctionnement d'autres composants ou éléments du SI. À titre d'exemple, des dysfonctionnements temporaires des logiciels des dossiers patients sont souvent prévus et vécus par les professionnels qui connaissent alors bien les procédures dégradées. Cependant, celles-ci peuvent s'appuyer sur un système de sauvegarde permettant d'accéder à une « photographie » du dossier patient prise peu avant le dysfonctionnement du logiciel, sans possibilité d'y effectuer des modifications, mais permettant de retrouver les prescriptions ou demandes d'examens en cours. Cet état des lieux peut se retrouver indisponible en cas de cyberattaque, en raison de l'indisponibilité des postes, du réseau informatique, ou des serveurs hébergeant ce plan de secours. Dans ce cas, la procédure dégradée est rendue immédiatement caduque en cas de cyberattaque et ne saurait irriguer le PCA, poussant à la recherche de nouvelles solutions.

Il convient donc, au-delà des informations que peuvent fournir les services, de confirmer la véracité de celles-ci auprès des services techniques et de vérifier qu'elles demeurent vraies dans le scénario retenu d'une cyberattaque totale. Une attention sera portée aux fonctionnalités ou activités qui sont assurées depuis un poste informatique et qui nécessitent une simple connexion internet. Ces activités sont souvent limitées voire inexistantes pour les services de soins, mais peuvent exister pour des activités de plateaux techniques, de rendus de résultats, ou de consultations d'informations (protocoles, procédures, etc.).

Concernant les communications, l'utilisation des moyens institutionnels risque d'être perturbée (téléphonie lorsqu'elle passe par le réseau, mail, etc.) sauf utilisation de moyens fournis par des opérateurs en dehors du réseau de l'établissement (Skype, Teams, etc.). L'utilisation de moyens non cautionnés par les pouvoirs publics (messagerie instantanée comme WhatsApp) reste à proscrire et ne peut être envisagée pour une communication de données médicales. Néanmoins, en temps de crise, l'utilisation de ces moyens peut être autorisée à titre exceptionnel. À titre d'exemple, l'AP-HP a ainsi reçu confirmation de l'autorisation, en cas de cyberattaque, d'utiliser ces moyens de communication non autorisés en conditions normales. Pour des raisons de confidentialité, ces moyens ne seront pas exposés ici.

2.1.6 Une fois les besoins évalués grâce à de premiers échanges avec les services, la recherche de solution, processus également chronophage, se basera sur une bonne connaissance des ressources de l'établissement

Cette recherche de solution doit être effectuée au niveau des métiers pour tous les processus qui n'impliquent que les métiers. Ainsi, les moyens de tenir des staffs, de réaliser des transmissions, ou de connaître la situation précise des lits devront être envisagés au niveau du service en fonction de son organisation, des schémas horaires, de la DMS et des ressources dont il dispose. Les solutions et les organisations varieront grandement en fonction de la taille et de la nature du service, un service d'urgence n'ayant pas les mêmes besoins qu'une unité de soins médicaux et de réadaptation avec une DMS de plusieurs semaines.

Dans la plupart des cas, des réponses locales pourront être trouvées pour proposer une première solution de continuité. Ainsi, les admissions peuvent a priori et en théorie être réalisées sans logiciel spécialisé, à partir d'une bureautique simple, voire sur papier.

Cependant, l'activité d'un établissement typique ne saurait être assurée sur papier plus de quelques jours selon les expériences des hôpitaux cyberattaqués. Si peu de problèmes sont rencontrés les premiers jours, les accumulations de papiers, dans des locaux qui ne sont plus forcément adaptés (salles d'archives par exemple), rendent difficile la traçabilité et la recherche d'informations produites. Il s'agit en réalité d'une constante dans le processus de conception des PCA : ne pouvant savoir à l'avance, et même une fois la crise survenue, combien de temps la situation sera amenée à perdurer, il devient nécessaire de prévoir des processus robustes ou à minima évolutifs (solution X du jour 0 au jour 3, solution Y du jour 3 au jour 15, solution Z à partir du jour 15) à même d'être maintenus des semaines, voire des mois.

De manière générale, si l'information doit pouvoir être retrouvée ou accédée plus d'une fois, y compris longtemps après sa production (cas des dossiers patients), il convient d'envisager un archivage numérique, ou de (re)mettre en place un archivage papier robuste et efficace pour chacune des activités qui utiliseront ce support.

Un usage de l'informatique reste néanmoins à privilégier. Une cyberattaque, même totale, détruisant les ressources physiques et numériques d'un SI ne signifie pas qu'il soit impossible d'utiliser des postes informatiques avant la reconstruction d'un système d'information. Les hôpitaux cyberattaqués ont ainsi systématiquement vu les professionnels venir avec leurs ordinateurs personnels ou dévaliser les magasins de matériel informatique

locaux afin de pouvoir assurer la traçabilité de leur activité par des outils de bureautique. Pour autant, un usage incontrôlé de matériel informatique non supervisé par la DSI au sein de l'établissement fait courir le risque de provoquer une surinfection numérique, en introduisant ou en réintroduisant des logiciels malveillants, voire la cyberattaque elle-même, dans un pseudo-SI officieux.

Ainsi, l'établissement doit pouvoir dresser un capacitaire de postes informatiques sains, à même d'être fournis par la DSI en cas de cyberattaque. Ces postes informatiques peuvent être détenus en propre par les établissements, détenus par des fournisseurs avec possibilité de déblocage rapide en cas de cyberattaque, ou commandables et livrables dans des délais très restreints. De ce capacitaire de PC de secours dépendent de nombreux éléments du PCA, permettant par exemple la fourniture de postes informatiques destinés à la gestion des activités des services.

Il ne s'agit pas là de proposer un plan de reprise de l'activité, qui s'inscrit dans une démarche de reconstruction d'un SI complet, mais bien de proposer aux services les moyens d'assurer certaines de leurs activités sur support informatique pour des questions de gestion de l'information qu'ils produisent eux-mêmes.

Ces postes informatiques peuvent également être absolument nécessaires dans les activités des plateaux techniques, particulièrement dans le cas de la biologie et de l'imagerie, qui ne peuvent, sauf rares exceptions, se passer d'informatique. Il faut donc faire la part des choses entre le matériel informatique critique, impérativement nécessaire à la continuité, et le matériel informatique destiné à la gestion qui peut être fourni à distance de l'attaque et non immédiatement après.

Sur ce sujet, et concernant les équipements biomédicaux, il convient d'adopter une stratégie différente de celle de la continuité des services de soins, dans la mesure où l'établissement est alors très dépendant de ressources externes et non propres à l'hôpital. En effet, l'existence de procédures dégradées à long terme, la capacité de certains de ces équipements à fonctionner sans le réseau de l'établissement, ou à produire des résultats (dans le cadre d'équipements de biologie et d'imagerie notamment) ne sont pas forcément connus des professionnels de l'hôpital. Ils peuvent néanmoins posséder certaines de ces informations et de bons contacts, commerciaux ou non, avec ces fournisseurs, facilitant l'obtention d'informations de leur part.

En raison du caractère presque externe de la démarche (peu d'établissements conservent des capacités propres importantes de gestion de leur parc biomédical), ou nécessitant à

minima un apport conséquent d'informations de la part d'acteurs externes à l'hôpital, cette étape peut être longue et nécessiter de nombreux échanges.

2.1.7 La recherche de solution techniques peut nécessiter des investissements ou des dépenses conséquentes, qu'il convient de faire arbitrer par un comité de pilotage et la direction générale de l'établissement

Si certaines des solutions de continuité qui vont être proposées ou trouvées peuvent être entièrement gratuites (développement d'outils en interne, usage nouveau de ressources existantes, simple réorganisation pérenne de certains processus pour diminuer la dépendance à l'informatique, réalisation de sauvegardes automatiques en dehors du SI de l'établissement ou sur des supports physiques), des dépenses restent inévitables. Il peut s'agir de matériel de secours, redondant avec le matériel existant, mais qui ne sera pas mobilisé pour s'assurer qu'il ne soit pas exposé à une cyberattaque.

À cet égard, il convient de préciser que la temporalité d'une cyberattaque peut être très longue, avec une première infection du SI plusieurs semaines, voire plusieurs mois avant le déclenchement de la cyberattaque. Dans ce cas, les matériels, données et sauvegardes réalisées sur le SI entre l'infection et la cyberattaque peuvent être rendus inutilisables, corrompus ou infectés, et doivent donc être détruits ou réinitialisés sous peine de repropager l'infection.

Ces matériels de secours ne peuvent donc pas être utilisés au quotidien, mais devront être stockés, représentant une immobilisation qui peut être coûteuse. Une solution consiste à augmenter le stock de matériels relativement consommables. Par exemple, un stock tampon peut être constitué au niveau des postes informatiques achetés par l'hôpital. Ainsi, l'on dispose en tout temps d'un certain nombre de PC non infectés à mobiliser en cas de cyberattaque, les PC nouvellement achetés venant peu à peu remplacer ce stock. Cette immobilisation représente un coût, aussi bien en immobilisation pure qu'en perte de temps sur la période de garantie des matériels. Il faudra également veiller à ce que ces PC disposent d'autres petits matériels afin de les rendre autonomes en temps de crise (clés 4G, disques de stockage supplémentaires, etc.). Il convient également de noter que l'enquête de l'ANSSI, qui survient systématiquement en cas de cyberattaque majeure, peut mener à l'immobilisation d'une quantité importante de matériel informatique, afin d'identifier l'origine de la cyberattaque. Cela concerne bien sûr les postes informatiques, mais également des équipements réseau et des moyens d'impression, pour lesquels il peut être utile de prévoir un stock stratégique mobilisable rapidement.

Cependant, certains matériels spécifiques ou plus coûteux ne peuvent pas être stockés par mesure de précaution au sein des hôpitaux, au risque d'immobiliser trop de ressources financières. C'est par exemple le cas de certains automates de biologie ou d'équipements lourds d'imagerie et de leurs équipements d'acquisition et d'analyse associés. À défaut, il convient de se renseigner auprès des fournisseurs sur le degré de vulnérabilité de ces appareils et sur la possibilité de les déconnecter du réseau dès lors que la cyberattaque est repérée afin de les préserver. Cette déconnexion, qui n'est pas toujours possible et ne sera peut-être pas utile si le matériel est infecté avant la détection de la cyberattaque, risque de perturber le fonctionnement de l'appareil, pour lequel une solution de continuité devra être trouvée.

La recherche de ce genre de solution peut être, en fonction du degré d'autonomie des interlocuteurs en question, laissée aux personnes en charge de ces équipements du côté de la direction ou bien du côté des services utilisateurs. Une approche de leur part est plus à même de permettre l'élaboration de solutions personnalisées, adaptées au contexte précis d'utilisation de ces équipements, et tenant compte des autres contraintes du PCA. Si certaines de ces prestations peuvent être réalisées gratuitement, certains fournisseurs les factureront. Il est également possible qu'aucune solution simple ne puisse être mise en œuvre sans investissement supplémentaire dans des équipements dédiés, et il conviendra alors de faire arbitrer l'opportunité de cet investissement en fonction de la criticité des processus et activités en question.

2.1.8 Le processus de recherche de solutions techniques ne doit pas s'autonomiser de la construction des PCA et des choix stratégiques établit par le pilotage stratégique du projet

Le haut niveau d'imbrication des processus au sein d'un établissement hospitalier, et le caractère en apparence sans fin de la réalisation des premiers PCA, ne doivent pas faire oublier le calendrier et le périmètre établis par le pilotage stratégique du projet. Il ne faut pas non plus oublier le caractère prioritaire de certains services ou processus. Ces premières orientations peuvent néanmoins être réajustées ou interchangées suite aux premiers BIA et aux premières recherches de solutions de continuité. S'engage alors un processus itératif d'aller-retour entre les niveaux stratégiques et opérationnels, largement guidé par les possibilités techniques et leur éventuel coût.

De surcroît, les ressources des services, des directions et de l'établissement en général sont limitées, tout comme le temps à consacrer à ce projet. Il est donc nécessaire de tenter de bâtir une forme de cohérence dans les arbitrages entre les différents PCA, d'identifier

les points communs, de veiller aux possibilités de mutualiser et d'étendre les réponses ou solutions trouvées localement à d'autres secteurs. Il ne faut pas perdre de vue non plus que ces solutions peuvent également reposer sur des échelons supra-établissement, au niveau du GHT, du territoire, de la région.

Dans ce contexte, l'arbitrage et la re-priorisation peuvent ne pas être aisés, et il faut alors revenir au but principal des PCA : continuer de soigner les patients.

Afin de disposer d'un comité de pilotage réactif, il n'apparaît pas concevable d'impliquer l'ensemble de la communauté médicale ou des représentants de chaque service. Il convient donc de désigner un petit nombre de responsables médicaux à même de gérer les priorités relatives des différentes prises en charge des patients. Ces capacités de priorisation sont essentielles afin d'éclairer les choix stratégiques du comité de pilotage. La création d'une ou plusieurs positions de Directeur médical de crise (DMC), ayant vocation à adopter ici une position stratégique, mais également opérationnelle en temps de crise, peut permettre de sacraliser ce rôle. En ce sens, le rôle apparaît à distinguer de celui de PCME.

2.1.9 Il convient de communiquer largement sur le sujet, afin de ne pas tenir à l'écart les services non sélectionnés, mais également de se saisir de ce projet pour aborder plus largement la cybersécurité

Le caractère limité des ressources à allouer à la construction des PCA écartera nécessairement une partie des services jugés moins critiques, qui pourront être abordés dans une seconde vague de PCA. Cela n'empêche pas ces services d'être destinataires d'une communication claire sur les enjeux du projet, sa méthodologie, et les grandes étapes et actions qui sont menées. Ils pourront également être destinataires des documents, fiches méthodologiques, et plus généralement des informations récoltées à l'occasion de ce processus.

Il faudra néanmoins s'accorder sur les informations qui seront transmises aux services, afin, par exemple, qu'ils ne se lancent pas seuls dans l'élaboration de leurs PCA, la recherche de solutions, voire l'acquisition de moyens, sans cohérence avec la stratégie établie. Des réunions de sensibilisation et d'information pourront être tenues afin de clarifier les attentes des directions vis-à-vis de ces services : attendre d'être embarqué dans le processus, commencer à réfléchir en interne au sujet, tenter de dresser un premier BIA, etc. De la même manière, il peut être intéressant d'aborder le sujet à travers les différentes instances de l'hôpital, afin que le sujet plus large de la cybersécurité puisse occuper une place plus importante dans les préoccupations de chacun.

Comme évoqué en première partie, les hôpitaux ont pu mettre un certain temps à atteindre un niveau désirable de sécurité sur leur SI. Malgré des montées en gamme importantes et une sécurisation apportée par les DSI de chaque établissement, le SI d'un hôpital reste vulnérable aux attaques en raison de son ouverture, aussi bien du point de vue de sa construction (un SI est à vocation à faire transiter l'information entre différents logiciels, services, usagers) que de ses utilisateurs. Un grand nombre d'attaques exploite les failles des usagers du SI et compte sur leur négligence numérique : techniques d'hameçonnage, dissémination de clés USB vecteurs de cyberattaques afin qu'elles soient branchées au SI du réseau, exploitation des accès des prestataires, …

La conduite d'un projet tel que la construction de PCA représente donc une bonne occasion de réaliser des diffusions institutionnelles abordant le sujet. Ainsi, des campagnes mails d'éducation à l'hameçonnage peuvent se montrer encore plus efficaces qu'en temps normal. Elles consistent en l'envoi, par la DSI, de mails à l'ensemble des agents de l'établissement qui imitent les techniques d'hameçonnage (par exemple, une adresse mail imitant celle de l'établissement à quelques caractères près, invitant à renouveler son mot de passe), et redirigeant les personnes cliquant sur le lien ou suivant les instructions vers une page visant à les informer sur leur échec face à ce test, et sur les précautions à prendre à l'avenir.

2.1.10 Le format des documents à produire n'est pas prescris, mais leur contenu doit être intelligible par le plus grand nombre

La plupart des cyberattaques d'ampleur sont volontairement déclenchées pendant des périodes où les capacités de réponse de l'établissement sont à un niveau bas. Les cyberattaques surviennent ainsi, presque traditionnellement, la nuit du vendredi au samedi, ou du samedi au dimanche, aux alentours de 2 heures. On observe également une augmentation de la fréquence des déclarations d'incidents numériques d'origine malveillante (tentatives de cyberattaque ou cyberattaques) à l'été et particulièrement en août.

Cela implique donc que les documents opérationnels de crise produits, surtout s'ils nécessitent la réalisation d'actions immédiatement après la découverte de la cyberattaque (déconnexion d'équipements du réseau pour les protéger, impression ou sauvegarde en masse de certaines informations clés comme les plannings d'intervention ou d'entrée de patients, ou encore les prescriptions en cours), doivent être accessibles, aussi bien physiquement qu'intellectuellement. Dès lors, les PCA produits doivent s'adresser non pas au chef de service, ni au cadre de service, mais bien aux personnes qui seront toujours présentes sur place (cadre de nuit, équipe soignante). Ils doivent fournir suffisamment de

détails pour des personnes qui connaissent potentiellement peu le service, mais suffisamment succincts pour être compris dans un moment de stress et de panique.

La déclinaison en de nombreux sous-documents doit être mûrement réfléchie, et chaque document doit, dans la mesure du possible, être autonome pour éviter de se perdre en recherche d'informations. Un document unique, détaillant les actions à prendre immédiatement et la conduite à tenir à très court terme (dans les premières 24, 48 voire 72 heures) constitue en cela un bon format. Il permet de ne contenir que les informations utiles pour le moment – et donc de produire un document succinct – et d'autonomiser les services de la cellule de crise qui ne pourra pas gérer en parallèle tous les services dans un premier temps. Des documents plus complets, détaillant la conduite à tenir et les solutions à mettre en œuvre à moyen terme, pourront être mis à disposition dans un second temps par la cellule de crise. Tous ces documents seront constitutifs du PCA de chaque service, la segmentation en une phase court terme et moyen terme visant à ne pas noyer les services dans une surcharge informationnelle. Cela tient aussi compte de l'évolution de la situation des services, qui seront très désorganisés et stressés (voire potentiellement avec un capacitaire réduit et peu d'encadrement en cas de survenue la nuit) durant les premières heures, mais plus à même de recevoir une information plus dense dès un ou deux jours.

Placer des indications physiques dans le service peut également être aidant, avec la mise en place d'une zone clairement identifiée ou de rangement abritant l'ensemble des documents et matériels nécessaires. Ainsi, le marquage des équipements à déconnecter (identification par un marquage coloré du câble à débrancher), couplé à un plan du service précisant leur emplacement, permet à toute personne, y compris extérieure au service, de mettre en œuvre les actions prescrites par le PCA sans connaissance supplémentaire.

Cette logique doit prévaloir dans le plus grand nombre de cas possible, bien que certaines opérations plus techniques ou nécessitant des connaissances préalables puissent ne pas se prêter à ce fonctionnement.

La réalisation de tests, y compris sur des éléments constitutifs du PCA et non le PCA complet, doit permettre d'éprouver leur contenu et de s'assurer de l'intelligibilité de l'information qu'ils contiennent, mais également de leur exhaustivité. Elle permet également aux agents du service de prendre connaissance de ces documents, et des exercices plus complets doivent également être menés avec les équipes de nuit.

3 Le caractère nouveau et bientôt obligatoire du sujet doit pousser les établissements à s'en saisir au plus vite

3.1 En tant que processus itératif et au long cours, il est préférable d'entamer précocement la démarche d'autant que des ressources intéressantes commencent à être mise en place

3.1.1 Le caractère nouveau et encore fluctuant mais aussi complexe de la cyber-résilience pousse à la création de postes dédiés

Comme évoqué en première partie, le sujet de la cyber-résilience des établissements sanitaires reste relativement nouveau, ce qui n'est pas nécessairement le cas des autres domaines, publics comme privés. Cela signifie notamment qu'il existe des personnes et des ressources capables de bénéficier d'une première expertise dans le domaine et qui pourraient être recrutées afin de structurer la démarche au sein des hôpitaux par la création de postes de chargés de crise ou de situations sanitaires exceptionnelles, dont font désormais partie les cyberattaques.

Par ailleurs, bien que le lancement des processus de création de PCA soit sans doute davantage consommateur de ressources que leur maintien, ces plans ont vocation à être vivants et à s'adapter aux évolutions au sein des établissements. Ils devront donc être mis à jour, régulièrement testés, et potentiellement revus et modifiés en profondeur pour tenir compte des évolutions opérationnelles et stratégiques de l'établissement.

Le caractère encore mouvant des appuis que peuvent fournir les autorités de tutelle ou les organismes dédiés au champ de la cybersécurité dans le domaine sanitaire, ainsi que le besoin de développement d'une forme d'expertise au sein des hôpitaux, plaident pour la création de postes pérennes. Une fois constituée, cette expertise pourra être mobilisée afin d'éclairer certaines prises de décisions stratégiques, touchant directement ou indirectement au sujet de la cyber-résilience, qui doit être distingué de celui de la cybersécurité, qui peut ne concerner que les DSI.

3.1.2 Le lancement de la construction des PCA risquant d'être complexe, il doit s'appuyer sur un comité stratégique solide, avec l'appui des directions et être porté par un acteur reconnu

L'absence de modèle et le caractère non linéaire de la démarche, ainsi que le très grand nombre de parties prenantes, nécessitent, en plus de l'éventuelle création de postes précédemment mentionnés, la mise en place d'une force de travail conséquente sous l'égide de la direction générale, épaulée par les directions fonctionnelles. Ces éléments

doivent s'incarner en une ou plusieurs personnes qui reprennent les caractéristiques évoquées en partie 2.1.4. Ce ou ces acteurs devront disposer d'une forte capacité organisationnelle, voire managériale, d'une relative disponibilité et autonomie, à même de traduire, par leur positionnement, le caractère de priorité stratégique qui aura été confié à ce projet, ainsi que d'une autorité reconnue et, si possible, d'une bonne connaissance des acteurs hospitaliers.

Tous les établissements ne pourront sans doute pas réunir l'ensemble des conditions, mais puisqu'il s'agit essentiellement d'animer une phase de lancement, avant une conduite du processus dans des phases itératives qui seront a priori davantage balisées, le recours aux élèves directeurs d'hôpital apparaît particulièrement indiqué afin de réunir ces compétences et ce positionnement. Le stage court constitue par ailleurs une période particulièrement appropriée pour établir les premiers contacts avec divers acteurs de l'établissement, apprendre certains rouages et cerner certaines dynamiques.

3.1.3 Le moment apparait également opportun afin de lancer la création de PCA qui est un processus au long cours

Comme évoqué précédemment, certaines aides financières, méthodologiques et même matérielles viennent de voir le jour, sont en cours de constitution ou vont être amenées à se développer. La période est donc propice pour bénéficier dès maintenant de ces aides, mais également éventuellement pour les infléchir, certaines d'entre elles devant être adaptées aux besoins des établissements.

La période est également propice à la structuration de partenariats, à la contractualisation et à la mutualisation avec un certain nombre d'organisations (autres établissements sanitaires du territoire, structures à même d'externaliser les examens de biologie ou d'imagerie, prestataires ou fournisseurs d'équipements ou de services) qui sont encore peu sollicitées dans le cadre de la résilience aux cyberattaques.

3.2 Le sujet des cyberattaques et de la cyber-résilience dépasse le seul champ informatique et doit irriguer un certain nombre de politique des établissements

3.2.1 Le sujet doit bien évidemment intégrer plus avant le domaine informatique en général

L'informatisation et la numérisation prennent une place croissante au sein des structures hospitalières, par exemple avec le développement des communications distantes (télé-

suivi, téléconsultation, téléexpertise, acquisition et transfert automatique de données) ou encore la dématérialisation des processus et des informations. Pour autant, bien que ce mouvement ait pu se faire pour des raisons d'efficience ou d'efficacité, mais aussi pour des raisons de qualité et de sécurité des soins, il convient désormais de juger de la pertinence de ce genre d'action ou projet à la lumière des potentielles faiblesses qu'il engendre.

De la même manière, les mouvements de mutualisation des moyens informatiques entre plusieurs sites ou établissements (mise en commun de réseaux, de serveurs, de logiciels, d'applicatifs, etc.) ont contribué à l'accroissement des vulnérabilités. Ces mouvements sont certes allés de pair avec un accroissement de la protection des systèmes et une montée en gamme des cyberdéfenses, mais il faut désormais s'interroger sur le compromis entre efficacité et/ou économies et les risques qu'ils font peser en termes de cyber-résilience.

3.2.2 Dans un mouvement contradictoire avec celui qui a pu être opérer, il peut être intéressant de développer à nouveau des formes de redondances dans les systèmes de gestion de l'information

Si la mise en commun de ressources a permis une rationalisation des moyens, elle diminue aussi la portée des secours ou mécanismes de sauvegarde. Ainsi, le passage progressif à des serveurs de stockage en réseau (NAS) a souvent éliminé les sauvegardes locales, ou l'usage de supports de sauvegarde physiques tels que les clés USB ou les disques durs. Si un retour à ces solutions alternatives n'est pas forcément souhaitable – de même qu'un retour au papier – car opérant dans des standards de sécurité bien inférieurs à ceux mis en place par les DSI, l'adoption de solutions de stockage à distance des données (cloud) peut être intéressante.

Elle permet par ailleurs de sous-traiter une partie de sa sécurité informatique, en confiant des données à des acteurs utilisant des mécanismes de protection, potentiellement meilleurs, et en tout cas différents, complexifiant ainsi la réussite d'une cyberattaque totale. Ces solutions sont néanmoins coûteuses, d'autant plus si elles ont vocation à héberger des données de santé. Dès lors, il convient de rationaliser les informations ou données qui seront stockées par ce biais, mais également leur fréquence de stockage. La mise en place de sauvegardes automatiques, sans manipulation de l'usager du SI, permet également de s'assurer de l'exhaustivité de l'opération.

Des solutions existent également pour proposer des sortes d'environnements numériques de travail, à même de proposer un certain nombre d'outils de bureautique et d'en sauvegarder les productions. L'intérêt de ces solutions est de ne pas héberger ni les outils (logiciels), ni les productions (documents) sur le SI de l'établissement, et d'en confier la

sécurité au fournisseur de la solution. À nouveau, ces solutions n'ont pas vocation à héberger des données de santé, mais restent très intéressantes dans la mesure où un poste informatique et une connexion internet sont suffisants pour y accéder et y travailler, constituant une solution de continuité bureautique en cas de cyberattaque.

3.2.3 La cyber-résilience s'entend également au-delà du seul champ informatique

Des domaines aussi divers que la politique d'achat, les contrats de maintenance, l'organisation des services et le choix de sous-traiter certaines compétences peuvent avoir un impact sur la cyber-résilience de l'établissement, ouvrant des brèches ou, au contraire, offrant des solutions de continuité.

À titre d'exemple, il serait donc intéressant d'intégrer lors de l'acquisition de certains équipements biomédicaux critiques, à minima, voire pour tous, des clauses de cyber-résilience. Elles viseraient à juger de la vulnérabilité des appareils en cas de cyberattaque, de leur capacité à fonctionner sans réseau, et des solutions proposées par les fournisseurs pour faire face en cas de cyberattaques. Des référentiels s'intéressant à ce sujet devraient voir le jour prochainement, comme celui à l'initiative de l'Association française des ingénieurs biomédicaux.

La sous-traitance de certaines fonctions ou compétences présente à la fois une force et une vulnérabilité, garantissant a priori une continuité de ces fonctions en cas de cyberattaque de l'hôpital, les prestataires n'étant pas concernés, mais empêchant parfois l'existence d'une expertise ou connaissance locale propre à l'établissement plus facilement mobilisable.

3.2.4 La cyber-résilience peut aussi passer par les usagers de l'établissement

Le développement du DMP permet en théorie d'accéder à l'ensemble des informations médicales d'un patient pourvu que celui-ci autorise le professionnel à y accéder. Cette source est accessible à tout professionnel de santé à jour de sa cotisation à son ordre et peut se faire indépendamment du réseau informatique de l'établissement. En tout état de cause, même une cyberattaque ne priverait donc pas les professionnels d'accéder aux antécédents médicaux, aux ordonnances et aux examens de leur patient.

Des mécanismes existent ou peuvent être mis en place afin d'assurer une bascule automatique des données produites par les établissements de santé sur les DMP de leurs patients. Ces bascules nécessitent cependant que l'identité des patients soit certifiée dans le SI de l'établissement (mécanisme de protection afin de s'assurer que les données produites sont affiliées au bon patient dans la base nationale que représente le DMP).

En plus de pouvoir travailler sur ces deux leviers (qualification des identités des patients dans le SI, bascule d'un maximum de données et documents sur le DMP), les établissements peuvent également sensibiliser les usagers à la prise en main et à l'alimentation de leur DMP, de manière à intégrer eux-mêmes certaines informations ou celles de leurs médecins de ville.

Cette sensibilisation peut également permettre de prévenir les usagers du risque de survenue de cyberattaque, rendant ainsi plus compréhensible la gestion de la crise une fois survenue.

Conclusion

Ces dernières années, les cyberattaques se sont multipliées, faisant de la cybersécurité une priorité pour les établissements sanitaires et leurs systèmes d'information, une préoccupation répétée depuis 2020 et le Ségur de la Santé, avec de premiers investissements majeurs dans le numérique. Le plan CaRE 2023-2027 a également vocation à renforcer les défenses des établissements en ce sens. Pourtant, le sujet de la cyber-résilience, qui commence à s'imposer en tant que tel, peine encore à se structurer pour le domaine sanitaire, alors que ce sujet est bien acquis dans d'autres domaines de l'État.

La tendance semble néanmoins en train de s'inverser avec l'achèvement d'une nécessaire montée en gamme des SI et de leurs défenses, ainsi que la création d'organisations, d'aides et de ressources visant à faire émerger un véritable plan blanc numérique. Alors que les premières mentions de ce terme mettaient encore trop l'accent sur la prévention, les initiatives récentes telles que la création des CRRC et l'obligation de créer des PCA dans la certification de la HAS visent davantage la réponse à une situation sanitaire exceptionnelle que constitue une cyberattaque.

Si les premières ressources produites sont à bien des égards imparfaites et insuffisamment opérationnelles, elles devraient s'améliorer à mesure des retours d'expérience des hôpitaux qui se lancent dans la création des PCA. Cependant, cela ne doit pas empêcher les établissements de se lancer dans ce sujet, qui représente également une opportunité pour l'hôpital. De plus, une prise de conscience trop tardive pourrait conduire à revenir sur certaines décisions prises par le passé (dématérialisation, suppression de toutes redondances qui pourraient représenter des points de sauvegarde ou des solutions de continuité), et empêcher la constitution d'une expertise locale rendue d'autant plus nécessaire que la numérisation et les obligations de cyber-résilience progressent.

Enfin, le développement d'une culture cyber, qui passe aussi par l'animation de sujets concrets au sein des établissements, constitue à la fois le moyen d'un dernier gain majeur en cybersécurité et un facteur de cyber-résilience. Elle permet à la fois de diminuer les risques de cyberattaque (en réduisant les risques de réussite par hameçonnage ou par intrusion physique dans le SI de l'établissement) tout en acculturant les professionnels, qui sont les premiers acteurs de la cyber-résilience, dans leurs pratiques ainsi que dans leurs souhaits d'organisation ou d'investissement.

En tout état de cause, le directeur d'hôpital, qui gère lui-même une direction fonctionnelle vulnérable aux cyberattaques et/ou la politique et la stratégie de l'établissement, doit lui-même se saisir du sujet afin de participer à sa diffusion.

Bibliographie

Référence juridique :

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

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

Article L. 6111-2 al. 1 du Code de la santé publique

Références administratives :

Guide d'aide à la préparation au volet numérique du Plan blanc note info DGOS 15 juin 2023

Guide pour réaliser un plan de continuité d'activité, Secrétariat général de la défense et de la sécurité national, 2013

Instruction n° DNS-2024-54 du 2 juillet 2024 relative aux missions des centres régionaux

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

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

Note d'information n° SG/SHFDS/2021/253 du 14 décembre 2021 relative à la mise en œuvre d'exercices cyber (PCA NUM) dans les établissements de santé

Note aux directeurs généraux des ARS du 30 juillet 2021 portant sur le Plan de renforcement 2021 de la cyber sécurité des établissements de santé

Note SHFDS-2021-40 aux directeurs généraux des ARS du 30 juillet 2021 portant sur le Plan de renforcement 2021 de la cybersécurité des établissements de santé

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

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

Guide d'hygiène informatique, version 1.0 de janvier 2013, ANSSI

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)

Introduction à la sécurité des systèmes d'information, guide pour les directeurs d'établissement de santé, publié en novembre 2013 par le ministère chargé de la santé

Publications :

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

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

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

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

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

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

Rapports :

Observatoire des incidents de sécurité des systèmes d’information pour les secteurs santé et médico-social 2023

Observatoire des incidents de sécurité des systèmes d’information pour les secteurs santé et médico-social 2022

Observatoire des incidents de sécurité des systèmes d’information pour les secteurs santé et médico-social 2021

Observatoire des incidents de sécurité des systèmes d’information pour les secteurs santé et médico-social 2020

Observatoire des incidents de sécurité des systèmes d’information pour les secteurs santé et médico-social 2019

Rapport public 2018 de l’Observatoire des signalements des incidents de sécurité des systèmes d’information pour le secteur santé sur la 1ère année de mise en oeuvre du dispositif (oct. 2017 – sept. 2018)

Webographie :

Ministère de la Santé et de la Prévention (sante.gouv.fr)

Agence nationale de la sécurité des systèmes d'information (cyber.gouv.fr)

CERT-FR – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ssi.gouv.fr)

Agence du Numérique en Santé | e-santé (esante.gouv.fr)

Groupement Régional d’Appui au Développement de la e-Santé (GRADeS) | G_NIUS (esante.gouv.fr)

Sesan - Service de santé numérique

LE JALU	Hugo	Octobre 2024

Filière Directeur d'Hôpital

Promotion 2023-2024

Cyberattaque, cyber-résilience et plans de continuité d'activité : Comment permettre à l'hôpital de continuer à opérer dès les heures qui suivent une cyberattaque

Résumé **:**

Alors que les cyberattaques se multiplient ces dernières années, la cyber-résilience des établissements de santé devient une priorité pour les pouvoirs publics.

Ce mémoire s'attache à présenter la menace à laquelle font face les établissements sanitaires, les défenses qui ont pu être mises en place, ainsi que la lente transition de la simple cybersécurité, propre aux DSI, vers la cyber-résilience qui concerne tout l'établissement.

Ce travail propose de répondre à la question suivante : « Quelle stratégie adopter pour construire des plans de continuité d'activité opérationnels permettant aux services de maintenir un haut niveau d'activité dans un temps contraint ? ».

Les ressources d'un établissement sont effectivement limitées, et la menace croissante des cyberattaques, tout comme l'obligation de mettre en œuvre des plans de continuité d'activité (PCA), imposent, sinon une finalisation, du moins un lancement rapide de ce processus.

Une approche opérationnelle, basée sur des acquis de terrain et confrontée à l'expertise d'acteurs du milieu hospitalier ou de la cybersécurité, est ici proposée afin d'initier la démarche et de disposer rapidement de premiers PCA pour un hôpital.

Ce champ encore nouveau, où des aides et accompagnements des autorités de tutelle et d'agences spécialisées viennent d'émerger, représente également une opportunité pour les établissements, qui gagneront à engager cette démarche le plus tôt possible.

Ce travail s'adresse à l'ensemble des directeurs d'hôpital souhaitant s'informer sur la démarche de création de PCA.

Mots clés **:**

Cyberattaque, cybersécurité, cyber-résilience, plan de continuité d'activité, PCA, système d'information, SI