Filière DH

Promotion : **2019-2020**

Date du Jury : **septembre 2020**

Le rôle du Directeur d'hôpital en matière de cybersécurité

Jean-Roch LETELLIER

Remerciements

Mes remerciements vont d'abord à l'équipe de direction de l'hôpital Edouard Herriot à Lyon, et à la Direction des Systèmes d'Information et de l'Informatique des HCL, qui m'ont accueilli durant mes stages et efficacement orienté vers les personnes susceptibles de répondre à mes questions.

Au premier rang de celles-ci, Mme Béatrice Bérard, OSSI des HCL, a apporté un éclairage technique, théorique, organisationnel, financier et managérial sur toutes les questions que je lui ai posées.

M. Philippe Benhaddou, de l'EHESP, a bien voulu me relire, commenter mon travail et partager la documentation et les contacts dont je pouvais avoir besoin.

Je remercie également M. François Sylvain, DSI du CHU de Rouen pour son analyse sur les événements qu'il a vécus et sa vision du rôle d'un Directeur d'hôpital dans une direction considérée comme technique.

Toute ma gratitude va, pour leur expertise en matière de gestion des risques, de gestion de crise, d'informatique, d'audit, de protection des données personnelles et de cybercriminalité, à MM. M. Bérard, L. Jamart, N. Ritouet et E. Trividic ainsi qu'au Commissaire F. Daviot et au Capitaine B. Perrier.

Je remercie MM. Ph. Loudenot et R. Rouxel pour l'intérêt qu'ils ont porté à ma démarche.

M. Chr. Vanderlinde a bien voulu, enfin, soutenir mon projet dès le départ, et me mettre en relation avec les personnes qualifiées.

S o m m a i r e

Liste des sigles utilisés

ABC : *Activity Based Costing*

AMRAE : Association pour le Management des Risques et des Assurances de l'Entreprise

ANS : Agence du Numérique en Santé

APSSIS : Association Pour la Sécurité des Systèmes d'Information Santé

APT : *Advanced Persistent Threat*

AQSSI : Autorité Qualifiée de Sécurité des Systèmes d'Information

CAIH : Centrale d'Achat de l'Informatique Hospitalière

CCH : Cellule de Crise Hospitalière

CIL : Correspondant Informatique et Libertés

CNIL : Commission Nationale Informatique et Libertés

CRRA : Centre de Réception et de Régulation des Appels

CTA-CODIS : Centre de Traitement des Appels – Centre Opérationnel Départemental d'Incendie et de Secours

(D)DoS : *(Distributed) Denial of Service*

DECT : *Digital Enhanced Cordless Telecommunications*

DICP/T : Disponibilité Intégrité Confidentialité Preuve / Traçabilité

DPI : Dossier Patient Informatisé

DPO : *Data Protection Officer*

DSI(I) : Direction des Systèmes d'Information (et de l'Informatique)

EDR : *Endpoint Detection and Response*

EENA : *European Emergency Number Association*

FSSI : Fonctionnaire de Sécurité des Systèmes d'Information

GAFAM : *Google / Amazon / Facebook / Apple / Microsoft*

GIE : Groupement d'Intérêt Economique

GTB /GTC : Gestion Technique des Bâtiments / Gestion Technique Centralisée

HCL : Hospices Civils de Lyon

HFDS : Haut Fonctionnaire de Défense et de Sécurité

IAM : *Identity Access Management*

IoT *: Internet of Things*

ISO : *International Organization for Standardization*

NIS (Directive) : *Network & Information Security*

OIV : Opérateur d'Importance Vitale

OSE : Opérateur de Services Essentiels

PCA/PRA : Plan de Continuité d'Activité / Plan de Reprise d'Activité

RGPD : Règlement Général sur la Protection des Données

RSSI : Responsable de la Sécurité des Systèmes d'Information

SCADA : *Supervisory Control And Data Acquisition*

SDN : *Software Defined Networking*

SGDSN : Secrétariat général de la défense et de la sécurité nationale

SGMAS : Secrétariat Général des Ministères des Affaires Sociales

SI(H) : Système d'Information (Hospitalier)

TCP/IP : *Transmission Control Protocol/Internet Protocol*

INTRODUCTION

Le contexte de la cybersécurité à l'hôpital : des risques nouveaux

Le principe selon lequel « on ne tire pas sur l'ambulance » a pu prévaloir au cours des conflits symétriques de l'époque contemporaine. A l'heure des conflits asymétriques, il n'est plus possible de s'en remettre à un quelconque « droit d'asile » pour considérer comme « sanctuarisés » les établissements de santé.

Le contexte géopolitique qui prévaut depuis vingt ans est celui d'une constante menace terroriste, à laquelle s'est ajoutée, en particulier sur le plan de l'affrontement politique, une menace étatique diffuse qui utilise souvent les moyens offerts par les outils cybernétiques dans un but de déstabilisation.

Dans le même temps, la collecte colossale de données requise pour faire fonctionner les systèmes d'information et en exploiter les possibilités a donné naissance à une nouvelle catégorie de prédateurs, dont le but est de mettre la main sur les données hébergées par les hôpitaux.

Le tableau d'ensemble de la situation est donc le suivant : les hôpitaux, privés comme publics, sont susceptibles d'être la cible

- d'attaques terroristes au sol,
- d'attaques cyber à motivation politique cherchant la déstabilisation des infrastructures sanitaires nationales,
- d'attaques à visée crapuleuse pouvant prendre différentes formes : le vol de données de santé avec l'objectif de les revendre, la paralysie d'un hôpital par la neutralisation de son système d'information à défaut du paiement d'une rançon.

L'actualité des dernières années a montré que cette menace n'était pas virtuelle :

- les hôpitaux ont, hors de France, été la cible d'attentats (en Afghanistan notamment) ;
- la main de certains pays est soupçonnée dans les attaques informatiques dont ont été victimes les hôpitaux britanniques en 2017, et les hôpitaux français en 2020.
- Les demandes de rançon formulées à l'occasion de l'attaque du CHU de Rouen en novembre 2019 et de celui de La Bassée (Nord) en octobre 2019, laissent à penser qu'une motivation financière est également à l'œuvre, sans qu'il soit permis de démêler exactement ce qui relève de la volonté de déstabilisation, et ce qui constitue à proprement parler une tentative d'extorsion.

Il est donc raisonnable de considérer que la cybersécurité dans les établissements de santé est devenue un enjeu de premier plan.

D'après les données les plus récentes[1], le nombre d'incidents d'origine malveillante est en augmentation légère, à 43%. En 2019, l'ANSSI a pris en charge 11 incidents, contre 2 en 2018 ; le HFDS en a suivi 14 (contre 6 en 2018) ; 392 signalements ont été réalisés (327 en 2018). Le nombre d'incidents qui auraient pu mettre en danger les patients est passé de 35 à 66.

Définir la cybersécurité

La cybersécurité peut se définir comme la capacité à protéger des données numériques. Cette protection prend différentes formes, qu'on résume en quatre exigences :

- D comme disponibilité : une donnée doit être accessible lorsqu'on en a besoin et que l'on est habilité à la manipuler ;
- I comme intégrité : une donnée doit rester elle-même, en fonction de sa destination. Elle ne peut être modifiée qu'à certaines conditions.
- C comme confidentialité : la donnée ne doit être accessible qu'à ceux qui ont le droit de la manipuler ;
- T comme traçabilité, ou P comme preuve : la donnée doit garder la trace des manipulations qu'elle a subies et de leurs auteurs.

Ces quatre exigences, souvent désignées par l'acronyme DICP ou DICT, consacrées dès 2005 par la norme ISO/IEC 27001[2], constituent les objectifs qu'une structure comme l'hôpital doit constamment garantir par rapport aux données, et *a fortiori* aux données de santé. En creux, on peut se représenter quels types d'incidents peuvent affecter les données : elles peuvent devenir inaccessibles, erronées, publiques ou incertaines. La cybersécurité consiste à faire en sorte que ces quatre risques sont contrôlés.

En croisant les différentes approches de la notion de la cybersécurité, on peut arriver à la typologie schématique des risques suivante[3] :

Types d'action		**Faille de sécurité**	**Victime**
Intrusion sur le système	Obtenir ou essayer d'obtenir un accès illicite à un système d'information ou à ses données	Confidentialité	Patients / institution
	Vol d'information		

[1] *Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur de la santé*, Rapport public 2019, Ministère des solidarités et de la santé, HFDS, ANS.
[2] https://www.iso.org/fr/isoiec-27001-information-security.html
[3] La liste des différents aspects de la cyber-attaque est tirée de *Cybersecurity : Guidelines and Best Practices for Emergency Services*, EENA, https://eena.org/wp-content/uploads/Cybersecurity-Guidelines-and-Best-Practices-for-Emergency-Services-1.pdf/

	Utilisation illicite d'un système informatique pour utiliser ou voler des données		
	Utilisation inappropriée de systèmes informatiques pour des agents, anciens agents ou sous-traitants.		
Action délibérée sur les données	Interruption involontaire ou déni de service, y compris la mise à l'arrêt de sites entiers ou d'autres services	Disponibilité	Patients
	Empêcher l'accès à un système ou à des données		
	Modifier la programmation d'un système d'exploitation ou de logiciels à l'insu de l'administrateur.	Intégrité	
	Altération des données ou adjonction de données falsifiées dans le système		
Modes d'accès	Installation de virus : codes ayant la capacité de contaminer rapidement un système d'information		Institution
	Effacement des traces laissées par l'attaque ; affirmation qu'elle n'a pas eu lieu	Preuve	

Ce tableau synthétique permet de rappeler les différents degrés d'une attaque, qui peut aller de l'intrusion quasi indétectable à une mise à l'arrêt retentissante du service. Dans le premier cas, on peut penser à l'attaque qui a visé la Direction Générale du Trésor et l'entreprise Areva en 2011 : un virus « taupe » a discrètement détourné et transmis des données pendant une période allant de quatre à dix-huit mois. Le deuxième cas est illustré par les événements de 2017 au Royaume-Uni ou ceux de Rouen en 2019.

La Direction des Systèmes d'Information et de l'Informatique aux HCL

Les HCL, par leur taille et les choix stratégiques faits assez tôt dans le développement des technologies numériques, constituent un terrain intéressant : le CHU de Lyon a une place à part dans le domaine de l'hôpital numérique puisqu'il est propriétaire et éditeur d'un DPI.

En 2009, en effet, des résultats financiers gravement déficitaires entraînent un plan ambitieux de rénovation et de recherche d'efficience. L'outil informatique utilisé alors, *Cristal-Net*, fruit d'une collaboration avec le CHU de Grenoble, n'est pas adapté pour faire face à l'exigence nouvelle imposée par la situation, et le choix de développer un outil propre est fait[4]. En 2012 est lancé une suite logicielle interne, *Easily*, qui va

[4] http://www.ticsante.com/les-HCl-deploient-leur-propre-suite-logicielle-hospitaliere-NS_1279.html

progressivement s'étoffer et être choisie par d'autres centres hospitaliers, d'abord dans la région Rhône-Alpes, puis au-delà. Le GIE Hopsis est fondé pour gérer le développement du logiciel *Easily* et les relations avec les établissements clients.

La DSII des HCL présente donc la particularité d'être aussi un éditeur de logiciel, ce qui en fait une direction particulièrement innovante, réactive – et par là même, hautement informée des enjeux et des défis de l'hôpital numérique. Un CHU aussi intégré et avancé en matière de SI que les HCL constitue donc un poste d'observation particulièrement adapté pour comprendre les enjeux actuels et futurs de la cybersécurité.

Problématique

Dans le contexte du développement conjoint du numérique et des menaces cyber, quelle est la place du Directeur d'hôpital, quelles sont ses responsabilités, et quels sont ses moyens d'action ? L'importance du sujet exige en effet que le *top management* s'en saisisse. Le présent mémoire a pour ambition de montrer ce que doit savoir le Directeur d'hôpital, même s'il n'est pas DSI, et surtout s'il est chef d'établissement. Pour ancrer dans le *management* cette approche de la cybersécurité, le choix a été fait de construire le plan autour des six verbes du *management* opérationnel[5] : **motiver**, **évaluer**, **développer**, **animer**, **organiser**, **diriger**.

La première partie sera consacrée à une présentation de l'état de la menace (*1.1. **Motiver** les managers de santé : faire prendre conscience du risque*). Il apparaîtra que cette menace est protéiforme, complexe à appréhender, et qu'en dépit de son caractère éminemment menaçant, les organisations hospitalières ne s'y sont pas encore totalement acclimatées (*1.2. **Evaluer** la maturité SI : comprendre d'où l'on part*).

La deuxième partie de ce travail évoquera les actions qu'il est possible de mener au regard de la législation : à partir d'une réglementation de plus en plus riche (*2.1 La réglementation de la cybersécurité*), le *manager* de santé doit entraîner ses équipes dans une démarche d'appropriation des outils *(2.2. **Développer** une culture de la cybersécurité : promouvoir la montée en compétence*) permettant de faire face à une attaque cyber (*2.3. **Animer** la montée et le maintien en compétence : s'exercer à des situations de crise cyber*).

La troisième partie envisagera d'un point de vue stratégique l'action du Directeur d'hôpital en montrant comment les organisations peuvent s'adapter afin de mieux tenir compte de la menace cyber (*3.1. **Organiser** le SI et son management : l'organigramme de la DSI*), et quels sont les enjeux financiers de la cybersécurité (*3.2. **Diriger** les évolutions et les soutenir : achat et budget*).

[5] Cours de management opérationnel de M. Bertrand Parent, EHESP, juin 2019.

1. COMPRENDRE LES ENJEUX DE LA CYBERSECURITE

La question de la cybersécurité se pose depuis que les Systèmes d'information hospitaliers sont connectés au réseau Internet, mais elle n'est l'objet d'un intérêt que sporadique de la part des futurs directeurs : seuls deux mémoires de la filière Directeurs d'hôpital répondent à la requête « sécurité informatique » dans la base de données de l'EHESP[6] depuis l'an 2000. Il est donc nécessaire de revenir sur la réalité de la menace cyber et son impact effectif ou potentiel sur les établissements de santé (1). Il est également indispensable de tenir compte du milieu professionnel particulier qu'est l'hôpital afin de comprendre, au moins en partie, les raisons du peu d'intérêt que suscitent les enjeux cyber (2).

1.1. Motiver les managers de santé : faire prendre conscience du risque

1.1.2 Campagnes de *ransomware* jusqu'au Covid

A) Etat de la menace : les groupes actifs

Se représenter la menace cyber qui pèse sur les hôpitaux nécessite de s'interroger sur les motivations de attaquants potentiels et les techniques d'attaque les plus employées.

a) Les attaquants et leurs motivations

La théorie de la cybersécurité, telle qu'elle est présentée par le SGDSN[7] ou l'ANSSI[8], distingue quatre profils d'attaquants potentiels, caractérisés par leur motivation :

- La déstabilisation
- L'espionnage
- Le sabotage
- La cybercriminalité.

La déstabilisation a pour moteur l'idéologie. Elle est le fait de campagnes d'hacktivistes qui, au nom de principes s'inspirant de la désobéissance civile, mènent des actions ciblées contre les cibles qu'ils ont identifiées. Les différentes campagnes A*nonymous* relèvent de cette tendance, ainsi que les *WikiLeaks* : il s'agit pour ces groupes de nuire, dans une démarche du faible au fort, à des entités nationales ou supranationales. Le

[6] Florence ARNOUX-LIOGIER, *L'émergence d'une politique de sécurité informatique au Centre Hospitalier Montperrin : jeux technico-organisationnels au croisement d'enjeux symboliques et matériels*, 2004 et Fabrice ORMANCEY, *La gestion du risque informatique à l'hôpital : protection de la confidentialité et sécurité des données au centre hospitalier de Dreux*, 2003.
[7] *Revue stratégique de cyberdéfense*, SGDSN, page 11, 2018
[8] https://www.ssi.gouv.fr/administration/principales-menaces/

secteur de la santé n'est, *a priori*, pas une cible prioritaire pour ces groupes. Leur mode d'action, qui met en péril l'activité de leur cible, risquerait de se retourner contre eux s'ils parvenaient à ralentir l'activité d'un hôpital par exemple. En revanche, on peut s'interroger sur la possibilité que des groupes de cette mouvance finissent, à l'occasion de débats nationaux sur le financement de la Santé, par utiliser les méthodes de « défacement »[9] pour appuyer leurs messages. On pourrait imaginer, par exemple, que la page d'accueil de grands établissements soit laissée active, mais caviardée par des bandeaux revendicatifs. Cette méthode n'a cependant pas été utilisée jusqu'à aujourd'hui.

L'espionnage consiste, contrairement à la déstabilisation, à attaquer discrètement afin de collecter des informations. Cette pratique ne concerne pas non plus le secteur de la santé, de prime abord, puisque les *process* médicaux, contrairement aux *process* industriels, ont plutôt vocation à être publics : les avancées de la science et de la médecine ne sont généralement pas considérées comme des secrets technologiques. Néanmoins, les hôpitaux hébergent bien d'autres informations qui, elles, peuvent être l'objet de convoitises relevant de la cybercriminalité plus que de l'espionnage. L'espionnage concernerait donc principalement, pour les hôpitaux, certaines fonctions précises qui auraient pour but d'alimenter un scenario d'attaque de plus grande ampleur : fonctionnement des réseaux électriques et de fluides, organisation de la téléphonie... En tant qu'OIV et OSE, un hôpital doit satisfaire à des obligations de sécurité concernant l'ensemble de ses approvisionnements, et peut donc, théoriquement, être la cible de manœuvre d'espionnage. Le cas n'est cependant pas renseigné.

Le sabotage est, lui, directement lié à la classification en OIV et OSE : certains établissements sanitaires ne doivent en aucun cas être contraints d'arrêter leur activité de dernier recours, ce qui induit que le sabotage est, pour eux, une menace. Les actions de sabotage consistent à empêcher l'activité primaire des hôpitaux, le soin. Les attaques dont des hôpitaux ont pu être victimes relèvent de cette catégorie lorsque les dossiers patients sont inaccessibles (*ransomware* et *cryptolocker*) ou que les sites sont saturés (*DDoS*). L'origine de ces attaques est toujours floue, comme on a pu le voir dans le cadre de la crise CoViD. Plus intrusive et lourde de conséquences qu'une action de *hacktivistes*, une campagne de sabotage impose à l'attaquant d'être furtif le temps qu'il installe son piège, et qu'il déjoue sans se faire repérer les dispositifs de sécurité. Le sabotage doit être considéré comme une attaque émanant d'un autre Etat plutôt que d'un groupe mu par une idéologie du fait de la complexité des attaques et de leur préparation. On peut en revanche tout à fait imaginer qu'une campagne de sabotage passe par des actions de déstabilisation et s'appuie sur une des manœuvres préliminaires d'espionnage.

[9] Les termes techniques sont expliqués dans le glossaire en Annexe 2.

La cybercriminalité constitue elle aussi une menace avérée : les hôpitaux sont des lieux de production de richesse dans la mesure où les données de santé sont des informations convoitées, et nécessaires à la prise en charge des patients. Jouer sur la disponibilité, l'intégrité ou la confidentialité des données de santé, en recourant au chantage, peut légitimement apparaître à des criminels comme une activité potentiellement rentable. C'est le sens qu'il faut donner au chantage à la restitution des accès au réseau dans le cadre d'un *ransomware*, mais les données peuvent aussi être volées puis revendues au marché noir. D'après les spécialistes, les liens entre sabotage et cybercriminalité peuvent être assez ténus, dans la mesure où une activité peut en cacher une autre.

Le caractère polymorphe des attaques peut être illustré par l'exemple suivant, concernant les équipements périphériques : on a détecté une faille dans les systèmes de climatisations utilisés par certains hôpitaux. Les climatiseurs peuvent être une porte d'entrée au réseau dans son ensemble pour une exfiltration de données, mais aussi servir à une action de sabotage en jouant sur la température des locaux[10].

La documentation est assez difficile à rassembler dans le domaine des attaques cyber car les victimes ne souhaitent pas être identifiées, et les services de l'Etat préfèrent enquêter discrètement. La déstabilisation est, en fait, à l'œuvre du moment qu'un soupçon pèse sur la fiabilité du système d'information d'un organisme. Renforcée par des campagnes de désinformation ou de *fake news*, une campagne de déstabilisation peut donc efficacement se transformer en action de sabotage, et les menées criminelles de groupes voulant faire un usage illicite de données volées concourent à la déstabilisation du système dès lors qu'une publicité trop complaisante en est faite. C'est ce que souligne l'ANSSI lorsqu'elle souligne que « La combinaison d'une attaque informationnelle (exploitation des réseaux sociaux pour amplifier) avec une attaque informatique maximise cette recherche d'atteinte à l'image."[11]

On peut représenter de la façon suivante les acteurs de la menace :

Catégories de pirates	Noms des acteurs	*Modus operandi*
APT (Advanced Persistent Threat) : nom générique des opérations de sabotage et de déstabilisation	**APT28** (Russie), repéré dans des attaques contre des laboratoires pharmaceutiques. Lazarus Group (Corée du Nord) Equation Group(USA) **APT41** (Chine), repéré dans des attaques contre des laboratoires pharmaceutiques.	*Phishing* puis acquisition de privilèges
Groupes de DoS (Denial of Service)	Lulzsec Lizard Squad Ghost Squad Hackers	Réseaux de *BotNets*

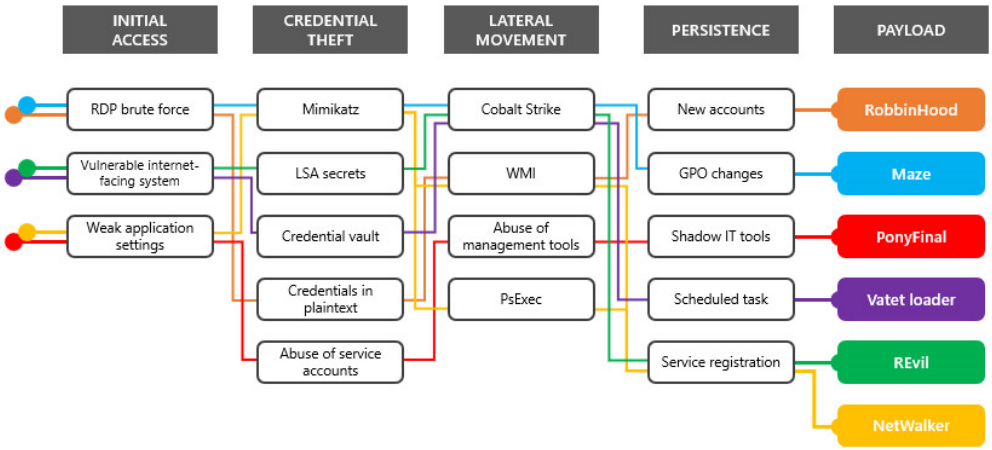
[10] https://www.zataz.com/des-hopitaux-et-grandes-enseignes-ne-protegent-pas-leur-climatiseur/
[11] https://www.ssi.gouv.fr/administration/principales-menaces/

	MCA DDoS Team	
Hacktivistes	Milworm Wikileaks Chaos Computer Club Anonymous	Réseaux de *BotNets*, DDoS, défacement
Les *insiders*	Les opportunistes Les employés mécontents Les maîtres-chanteurs Les traitres	Utilisation d'identifiants valides et d'accès légitimes pour voler des données ou infecter les systèmes.
Le crime organisé, les cybercriminels	TRM Dark Hotel Carbanak Fin7 Morpho/Wild Neutron Group	N'importe quelle méthode – le *phishing* est souvent une voie d'accès efficace.
Les hackers patriotes	Syrian Electric Army (Syrie, pro-Bachar el-Assad) Tarh Andishan (Iran) Guccifer 2.0 (origine russe soupçonnée) The Jester (Peut-être USA)	

Tableau réalisé à partir des données *Radware*[12] et *Orange CyberDefense*

b) Les techniques d'intrusion et de piratage

Le schéma suivant, proposé par Microsoft[13], permet de mettre en évidence l'état de la menace à une date récente (28 avril 2020).



Sur la droite, la charge virale est désignée par son nom « commercial » et public. Les étapes qui précèdent illustrent la méthode de chaque virus pour entrer dans un réseau (*initial access*) et pour se procurer des identifiants existants (*credential thefts*). Ensuite, le pirate a les ressources suffisantes pour gagner des privilèges supplémentaires par

[12] *Hacker's Almanac : a field guide*, Radware, 2019, disponible sur https://www.radware.com/hackers-almanac/

[13] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

mouvement latéral (*lateral movement*) et atteindre une situation qui permette à la charge virale d'avoir le plus gros impact possible. A partir de ce moment, le pirate est en mesure d'agir sur le réseau (*persistence*) avec les privilèges les plus élevés en utilisant plusieurs méthodes :

- La création d'un nouveau compte,
- La modification de l'*Active Directory* par des changements de *Group Policy Object*s (GPO)
- Les outils de *Shadow IT*, qui permettent d'agir sur les logiciels métiers en contournant la supervision de la DSI
- La création de tâches s'effectuant automatiquement.

La liste de virus présentés ici n'est pas exhaustive, et d'autres, tels que *Sodinokibi* ou *Ragnar*, ou encore des consortiums tels que *Ragnar-Maze*[14] utilisent conjointement différents modes d'attaque.

Un autre classement des groupes de pirates en fonction de leurs techniques d'attaques permet de se représenter l'état de la menace actuelle :

Type d'attaque	Nom des pirates / de la charge virale	Voie d'abord habituelle
Botnet	Necurs Mirai Brickerbot **Trickbot** (activité avérée pendant la crise Covid)	Faiblesse des identifiants Failles des objets connectés
Outil de test	Coin Miner Defcon.pro **Remcos Rat** (activité avérée pendant la crise Covid) Kali Linux	Ces outils ont pour vocation de tester les défenses d'un réseau et adapter sa sécurité : ils peuvent donc aussi être utilisés de façon offensive.
Défacement	Error squad Electronic Thunderbolt Team Giant's-PS Anonplus	Failles non réparées Prise de contrôle à distance Injections SQL
Kits "exploits"	Magnitude exploit Kit Grandsoft Exploit Kit Terror Exploit Kit Rig Exploit Kit	Ces "kits" permettent d'obtenir des informations sur une faille non corrigée.
Ransomware	**Wannacry** (Attaque contre le NHS en 2017) **Notpetya** (Attaque en 2017 contre les laboratoires pharmaceutiques Merck & Co) **Samsam** (Deux hôpitaux américains ciblés en 2018) Locky	Campagnes de *phishing* *botnets*

[14] https://www.zataz.com/quand-les-operateurs-de-ransomware-sunissent/

	Maze (dit ne pas s'attaquer aux établissements sanitaires[15])	
Cheval de Troie	Tinyloader Zeus **Emotet** (activité avérée pendant la crise Covid) Kovter	Ingénierie sociale Dissimulation dans un logiciel sain

Tableau réalisé à partir des données *Radware*[16] et *Orange CyberDefense*[17], [18]

Des failles touchant les systèmes ne cessent d'être découvertes, et peuvent entraîner une vulnérabilité très large des outils utilisés. A titre d'exemple, la presse spécialisée a annoncé le 17 juin 2020 que dix-neuf failles affectant le protocole TCP/IP[19], c'est-à-dire le protocole le plus utilisé du réseau, avaient été repérées par un groupe israélien d'analystes en cybersécurité, JSOF[20].

B) Les données personnelles, nouvel objet de convoitise

a) La protection des données

L'autre aspect de la question de la mise en sûreté des systèmes d'information concerne la protection des données personnelles, considérées comme proie tentante par certains acteurs économiques. De ce fait, le partage d'informations rendu possible par la mise en place de dossiers patients informatisés – partage dont bénéficient chaque jour les patients des établissements de santé grâce à la souplesse de l'outil – a été strictement borné par le législateur à un usage médical en lien direct avec le patient par **l'article L 1111-13-1, IV-3[21] du Code de Santé Publique**. Sylvie Hennion explique de la façon suivante cette limitation de la transmission des données :

> « le champ contractuel est formellement exclu du partage de données, qu'il s'agisse des contrats de protection sociale complémentaire dûment précisés, mais aussi de tous contrats d'assurance, de prêt, contrat de travail ou de consommation. Les typologies de contrats sont multiples et les informations de

[15] *The Threat of Cyberattacks on healthcare establishments during the Covid-19 pandemic*, Orange Cyberdefense Epidemiology Lab, OSINT Unit, 20 mars 2020, page 3
[16] *Hacker's Almanac : a field guide*, Radware, 2019, disponible sur https://www.radware.com/hackers-almanac/
[17] *The Threat of Cyberattacks on healthcare establishments during the Covid-19 pandemic*, Orange Cyberdefense Epidemiology Lab, OSINT Unit, 20 mars 2020, page 7
[18] *Potential risks for the pharmaceutical sector*, Orange Cyberdefense Epidemiology Lab, OSINT Unit, 29 avril 2020
[19] https://www.healthcareinfosecurity.com/millions-connected-devices-have-exploitable-tcpip-flaws-a-14451
[20] https://www.jsof-tech.com/ripple20/
[21] « La communication de tout ou partie des données de l'espace numérique de santé ne peut être exigée du titulaire de cet espace lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et lors de la conclusion ou de l'application de tout autre contrat, à l'exception des contrats relatifs aux services et outils numériques référencés en application du III du présent article »

santé, à l'heure de l'intelligence artificielle, ne doivent pas entraîner un commerce de santé prédictive dont tous les acteurs économiques pourraient être friands. »[22]

La limitation de la transmission des données entraîne *de facto* la constitution d'un marché noir de ces données de santé, qui peuvent, sur les espaces clandestins du *darknet,* atteindre des prix supérieurs à ceux des données bancaires[23].

b) Le détournement des données

L'emploi indu de ces données peut en effet, comme le laisse entendre le texte de loi, avoir un impact sur le montant des primes d'assurance exigées par les patients, mais il peut trouver aussi d'autres débouchés, que ce soit dans la fixation des tarifs des médicaments par ciblage fin des catégories de malades ; de façon plus brutale encore, l'emploi des données de santé peut permettre, par des recoupements entre le type de soin et le degré de couverture santé, de construire des bases de données de personnes à haut revenu susceptibles d'être visées efficacement par des manœuvres d'extorsion ciblées : la tendance actuelle de la piraterie informatique est au *big game hunting*, « chasse au gros gibier » qui délaisse les attaques indiscriminées et peu rentables au profit de bons payeurs potentiels, harponnés par des campagnes de *spear-phishing*, ou *phishing* ciblé. C'est dans cette perspective qu'on doit analyser la montée en puissance, en fréquence et en intensité des attaques contre les établissements de santé.

Le dernier avantage des données de santé, par rapport aux données bancaires, est que le voleur peut les utiliser de façon bien plus durable : si un mouvement suspect sur un compte en banque peut être très rapidement identifié par la victime, il n'en va pas de même pour des données présentes sur la Carte Vitale. Une victime de divulgation de données aura tendance à découvrir par hasard, parfois longtemps après, la rupture de confidentialité.

c) Données et IA

Les données de santé, enfin, sont le carburant des algorithmes utilisés par les chercheurs en l'intelligence artificielle, qui sont tous, pour les plus importants, des acteurs privés à but lucratif. Le club de ces acteurs aux puissances de calcul et de stockage incomparables est très fermé : c'est celui des GAFAM, qui se lancent sur le marché de la santé en profitant de son caractère extrêmement porteur. D'après le Pr. Philippe Ravaud, cité dans un article du *Monde*,

---

[22] Sylvie Hennion, « le partage du secret professionnel à l'heure du numérique », RDSS, janvier février 2020, p 144.

[23] Caroline Humer, Jim Finkle*, Your medical record is worth more to hackers than your credit card*, Reuters, 24 septembre 2014, disponible sur https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

> « Les GAFAM ne peuvent pas générer de la donnée profonde de santé comme un CHU, mais ils négocient massivement pour en acquérir. Ils ont de l'argent, de la matière grise et une capacité à investir quelle que soit la prise de risque. Sur vingt projets, peut-être qu'un seul marchera, mais il suffira à financer tout le reste. »[24]

Dans ce cas, les données de santé sont collectées sans but particulier *a priori* : c'est dans la masse des données qu'une IA trouvera ou non des constantes, des éléments prédictifs ou des exploitations pratiques diverses[25]. A l'heure actuelle, l'objectif est la thésaurisation, et le volume des données s'accroît de façon exponentielle.

d) Données et Cloud

La centralisation des données, en France, au sein du *Health Data Hub* hébergé par Microsoft pose donc des questions réelles de confidentialité. Quelles que soient les assurances données par la société américaines, en effet, il est prudent de considérer que toute donnée qui lui est confiée est susceptible de tomber sous le coup du *Clarifying Lawful Overseas Use of Data Act*, ou *Cloud Act*, de 2018 : selon Marie-Laure Denis, Présidente de la CNIL,

> « Cette loi facilite un accès direct par les autorités américaines aux données stockées hors du territoire américain dans les cas ne relevant pas d'une procédure judiciaire classique, et assure une réciprocité pour les autorités européennes »[26]

Par conséquent, il est permis de s'interroger sur la fiabilité du recours à une entreprise comme Microsoft pour le stockage des données de santé françaises, étant donné l'aisance avec laquelle les Etats-Unis usent des procédures extraterritoriales et n'hésitent pas à privilégier leurs entreprises.

e) La fuite des données : un risque réel

Un des grands enjeux de la gouvernance hospitalière est donc, pour les années à venir, de prendre la mesure du risque cyber, de s'y préparer et d'inventer les parades à une attaque de ce type. Si, statistiquement, les attentats au sol sont spectaculaires, terrifiants, et justifient une mise en sécurité adaptée des établissements de santé, la probabilité d'une attaque cyber est dramatiquement plus élevée : 10 à 15% des EPS sont touchés

[24] Laure Belot, "Les données de santé, un trésor mondialement convoité", *Le Monde* du 2 mars 2020.
https://www.lemonde.fr/sciences/article/2020/03/02/les-donnees-de-sante-un-tresor-mondialement-convoite_6031572_1650684.html
[25] L'assureur SHAM, par exemple, a conclu un accord avec la société d'IA *Caresyntax*.
[26] *Compte rendu de la Commission des affaires européennes*, Audition de Mme Marie-Laure Denis, Présidente de la commission nationale de l'informatique et des libertés (CNIL), 27 juin 2019, disponible sur http://www.assemblee-nationale.fr/15/pdf/europe/c-rendus/c0099.pdf

par des tentatives d'attaque chaque mois, et on dénombre en moyenne 27 attaques chaque mois[27].

Le coût enfin d'une attaque informatique peut être particulièrement élevé. Dans un hôpital, le coût financier d'une attaque réussie, à court terme, serait composé par :

- Le temps d'interruption des services
- La perte (éventuelle) des données d'activité non transmises
- Le temps de contrôle des équipements et de remise en route, ou le remplacement du parc entier des équipements terminaux.

A ces coûts directs s'ajouteraient ceux liés à la perte de réputation et, éventuellement, au risque juridique.

1.1.3 La crise sanitaire du printemps 2020

Toutes les crises majeures constituent, pour les cybercriminels, une incitation à tirer parti de la situation en profitant du manque de vigilance et du relâchement des procédures justifié (ou non) par l'urgence. La crise sanitaire de 2020 a illustré cette fragilité des organisations dès lors qu'un événement exceptionnel est en cours.

A) Les attaques informatiques durant la crise du coronavirus

Dans le cas de la pandémie de CoViD 19 de 2020, la lutte contre le virus biologique s'est doublée d'une lutte contre une épidémie d'attaques informatiques à grande échelle, ayant touché spécifiquement les structures sanitaires des pays occidentaux. Pour le seul mois de mars 2020, on dénombre ainsi une attaque contre l'Organisation Mondiale de la Santé, OMS, par le biais de sa messagerie interne, une autre contre le ministère de la Santé américain, une autre encore contre l'hôpital universitaire de Brno en République tchèque, qui a ralenti fortement le traitement des résultats des tests de contamination, et une attaque DDoS contre l'AP-HP, qui a imposé un redémarrage de l'ensemble du système d'exploitation, avec les retards afférents.

Malgré la difficulté qu'il y a à établir précisément l'implication d'acteurs définis, les spécialistes ont identifié dans le cas des attaques contre l'OMS et le ministère américain des groupes de hackers affiliés au régime chinois pour l'une (le groupe APT41[28]), et au régime nord-coréen pour l'autre. Le caractère global de cette menace se confirme début

[27] Dossier d'information « tous cyber vigilants », novembre 2019
[28] "While APT41 is a unique state-sponsored Chinese threat group that conducts espionage…", https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

avril, avec la diffusion d'une « note mauve » d'Interpol alertant sur la détection de *ransomwares* s'attaquant à des établissements de santé partout dans le monde[29].

Si toutes les tentatives de *phishing* n'ont pas été réussies, leur nombre a de quoi inquiéter, ainsi que leur caractère rudimentaire : les pirates, jouant sur l'émotion et l'hypersensibilité générale à tout ce qui concernait la lutte contre le virus Sars-Cov-2, se sont contentés de procéder par la mise en valeur de mots clefs jouant le rôle de *clickbaits* comme « vaccin », « virus » « chloroquine » etc.

B) La santé publique au carrefour d'enjeux géopolitiques

Ces attaques directes contre des structures chargées de lutter contre la pandémie ne sont, au demeurant, qu'un des aspects de la lutte qui se joue dans le cyberespace : des campagnes de propagande sont également menées pour affaiblir les choix politiques faits par certains pays, ou promouvoir les qualités prêtées à la gestion de la crise dans d'autres pays. La ligne de fracture est assez nette : les campagnes agressives d'information tendancieuse ont toutes pour objet de saluer l'efficacité de la politique menée par Moscou ou Pékin[30], sans que ces pays n'autorisent à mesurer l'ampleur prise par la pandémie chez eux. Au contraire, les politiques menées par les pays occidentaux sont critiquées violemment et assimilées à divers « complots » pour le moins fumeux. Les journalistes Mathieu Suc et François Bougon relatent ainsi, dans un article du 29 mars 2020 dans *Mediapart*, que des sources du milieu du renseignement leur ont fait part de

> « leur courroux vis-à-vis d'opérations menées par différents États, surfant sur le complotisme ambiant à propos de l'origine du virus pour mener des campagnes de désinformation, manipuler l'opinion publique et critiquer l'action des autres gouvernements, taxés d'incompétence en contraste avec l'efficacité vantée de leurs régimes autoritaires. »[31]

Dès lors, il est permis de considérer que les cyberattaques dont sont victimes des établissements de santé et les organismes nationaux de santé publique peuvent, pour une part au moins, faire partie de cette ambition de déstabilisation de pays comme la France au profit de régimes autoritaires, à la fois pour renforcer leur légitimité intérieure, et pour affaiblir les démocraties. C'est le sens de la note du Service Européen pour l'Action Extérieure, SEAE, du 16 mars 2020, citée par le *Financial Times* :

---

[29] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Des-cybermalfaiteurs-lancent-des-attaques-par-rancongiciels-contre-des-etablissements-de-sante-essentiels

[30] Ces deux pays sont nommément cités dans un rapport de la Commission européenne du 10 juin 2020 : https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_fr

[31] https://www.mediapart.fr/journal/international/290320/en-pleine-pandemie-une-ambiance-de-guerre-froide?utm_source=article_offert&utm_medium=email&utm_campaign=TRANSAC&utm_content=&utm_term=&xtor=EPR-1013-%5Barticle-offert%5D&M_BT=2067267294978

> « The overarching aim of Kremlin disinformation is to aggravate the public health crisis in western countries, specifically by undermining public trust in national healthcare systems — thus preventing an effective response to the outbreak. »[32]

Le caractère contre-productif de cette stratégie, si elle est avérée, peut néanmoins s'expliquer si l'on se réfère aux analyses de Soraya Sidani sur la « déviance normative ». Il s'agit en effet, pour des pays à qui des retards socio-économiques interdisent d'être sur un pied d'égalité avec les grandes puissances internationales, de jouer un rôle d'acteur incontournable et de proposer une alternative viable.

> « Entre contraintes d'intégration et logiques de puissance, les États en marge du système révèlent ainsi les faiblesses d'une structure internationale qui peine encore à assembler ses composantes les plus diverses et à abolir les stratégies de domination des États les plus puissants. »[33]

Ces lignes, lues au regard de la situation chaotique engendrée par la crise de la CoViD 19 et de la désorganisation globale des pays pour faire face à la pandémie, sont particulièrement éloquentes : un Etat en marge a, en l'occurrence, tout intérêt à faire preuve de sa spécificité et de sa résistance par rapport à des pays intégrés au système démocratique et dont la réactivité face à la crise est manifestement mise en défaut. Intervenir directement en nuisant de façon délibérée au fonctionnement des systèmes d'information, grâce à des cyberattaques, et en alimentant une défiance populaire vis-à-vis des pouvoirs publics constitue donc une stratégie cohérente.

Dans le cas particulier de la crise sanitaire, le « front » cyber est donc double : il est constitué à la fois de la couche logique (celle de l'attaque informatique proprement dite, qui met à mal un SI) et de la couche sémantique, celle du contenu des informations échangées et relayées. La prise de conscience de cette menace par le *top management* hospitalier est une nécessité.

---

[32] "EU warns of pro-Kremlin disinformation campaign on coronavirus" par Michael Peel et Sam Fleming, Financial Times du 17 mars 2020, https://www.ft.com/content/d65736da-684e-11ea-800d-da70cff6e4d3

[33] Sidani Soraya, « Introduction », dans : Intégration et déviance au sein du système international. Paris, Presses de Sciences Po, « Relations internationales », 2014, p. 17-28. URL : https://www.cairn.info/integration-et-deviance-au-sein-du-systeme-interna--9782724615708-page-17.htm

1.2 Evaluer la maturité SI : comprendre d'où l'on part

1.2.1 Les soignants et la sécurité

A) Une menace intérieure : l'absence de prise de conscience

Quel que soit corps de métier, la compréhension des impératifs de cybersécurité et de la responsabilité individuelle pour sécuriser un réseau est insuffisante. A partir de ce constat, la fuite de données est inévitable et relève beaucoup moins de l'ingéniosité du voleur que de la maladresse de sa victime. Selon le rapport 2019 de *Verizon* sur la fuite de données dans tout type de structures[34], les erreurs et mésusages sont présents dans un tiers des incidents concernant des données ; assez logiquement, les fuites ont pour origine, dans 34% des cas, des agents de la structure elle-même. Dans le secteur de la santé, ces erreurs diverses et abus de privilèges d'accès expliquent 81% des fuites de données, et la menace vient, à 60%, de l'intérieur des structures de santé. Le mauvais adressage des mails, la publication intempestive de données confidentielles sont les sources majeures de divulgation. On trouve le même constat dans nombre d'autres publications portant sur la cybersécurité : « Poorly trained staff is one of the main reasons for cybersecurity breaches » selon l'EENA[35].

Les attaques proprement dites existent, et sont menées majoritairement sous la forme du *phishing*, qui joue sur le *social engineering* : autrement dit, c'est encore l'erreur humaine qui est à la base des fuites de données. Cette fragilité des systèmes entretenue par leurs utilisateurs quotidiens est renforcée par un faux sentiment de sécurité : pour la plupart des agents, la sécurité informatique est assurée par la DSI et l'on n'a, par conséquent, pas à s'en préoccuper – de la même manière que, dans le cadre d'un usage personnel de l'informatique, l'existence d'un antivirus apparaît à la plupart des utilisateurs comme une condition à la fois nécessaire et suffisante à la sécurisation des données personnelles.

Dans ces conditions, la première étape pour sécuriser un système d'information est, à l'évidence, une campagne large et itérative de formation sur les fragilités du système.

B) Le rapport des soignants à la sécurité

Par ailleurs, les personnels soignants peuvent avoir vis-à-vis des domaines perçus comme relevant de la sécurité une certaine défiance. Les cultures professionnelles respectives des soignants, d'un côté, et de l'autre, des acteurs de la sécurité sont très fortes et parfois difficilement compatibles. Du côté des soignants, la volonté de

[34] 2019 Data Breach Investigation Report, Verizon

[35] *Cybersecurity : Guidelines and Best Practices for Emergency Services*, EENA, https://eena.org/wp-content/uploads/Cybersecurity-Guidelines-and-Best-Practices-for-Emergency-Services-1.pdf/

promouvoir au maximum les soins peut s'accompagner, parallèlement, d'une volonté de mettre au second plan les contraintes liées à la sécurité. En conséquence, toute intrusion d'enjeux considérés comme sécuritaires dans les procédures liées aux soins est susceptible d'être envisagée avec circonspection. Les thématiques liées à la sécurité informatique étant en partie liées à des missions de sécurité intérieure, il n'est pas évident *a priori* de faire accepter par certaines équipes soignantes une culture vue comme étrangère. Ce constat, au demeurant, n'est pas vrai pour tous les services et spécialités : ainsi, les services d'urgences ou le SAMU, en contact régulier avec les forces de l'ordre, sont plus susceptibles d'intégrer les contraintes de sécurité que les services d'hospitalisation conventionnelle.

En 2014, l'éditorial du dossier « Hôpital et police » de *Gestions hospitalières* commençait de la façon suivante :

> « Les relations entre les services publics que sont la justice, les polices nationale et municipale, la gendarmerie et l'hôpital sont quotidiennes et fondées sur un ensemble juridique complexe soumis à l'interprétation d'acteurs opérationnels motivés par une formation, une culture, des méthodes parfois sources d'incompréhension. Pourtant, tous poursuivent l'objectif commun de protection des personnes et sont interdépendants. La clarification partagée et formalisée des procédures d'intervention et leur validation hiérarchique contribuent à simplifier, à pacifier les relations. La reconnaissance mutuelle des contraintes et obligations de chacun permet d'agir sereinement sans remise en cause des valeurs. »[36].

Derrière le lexique positif et optimiste qui décrit les relations entre police et hôpital, on perçoit nettement, en creux, les difficultés de cette collaboration : la question du conflit de valeurs et de cultures continue nécessairement d'exister, six ans après que ces lignes ont été écrites, même si les événements dramatiques de 2015 et 2016 ont pu faire évoluer les mentalités. Certains équipements de sécurité, tels que des dispositifs anti-tuerie de masse, commencent à être installés dans les hôpitaux. Il est peu probable que de telles mesures eussent pu être prises avant la vague d'attentats de 2015-2016.

Il n'en demeure pas moins que l'application de contraintes de sécurité intérieure au milieu hospitalier ne peut se faire de façon entièrement fluide, et que la culture de la cybersécurité, identifiée à une culture de sécurité intérieure, requiert un effort particulier de sensibilisation. Pour illustrer cette évolution des cadres de référence, on peut rappeler que, jusque dans les années 2000, les méthodes de cryptographie relevaient sur secret militaire – elles sont aujourd'hui utilisées dans n'importe quelle conversation *WhatsApp*.

[36] *Gestions hospitalières*, Numéro 540 - novembre 2014

1.2.2 Le rapport des Directeurs d'hôpital à la cybersécurité

Partant du principe que les Directeurs d'hôpital, appelés à jouer le rôle d'AQSSI (Autorité Qualifiée de Sécurité des SI) devaient devenir des acteurs de la cybersécurité, j'ai mené auprès de mes collègues Directeurs stagiaires et de Directeurs en poste une enquête portant sur leur vision du rôle du Directeur en matière de cybersécurité. Cette enquête avait pour objectifs :

- de mesurer l'intérêt que portent les DH et futurs DH à la cybersécurité, et la représentation qu'ils se font de ses enjeux ;
- de constater leurs connaissances en la matière, à la fois en termes de technique et de réglementation ;

Menée par l'intermédiaire d'un formulaire *Microsoft Form* en ligne entre le 4 juin et le 4 juillet 2020, cette enquête anonyme a obtenu 44 réponses, dont 7 émanant de directeurs en poste. 70% des personnes ayant répondu sont rattachées à un CH, les autres à un CHU. Cependant, cette variable ne laissait pas apparaître de variation notable dans les réponses.

A) Un intérêt théorique pour la question

Le résultat de cette enquête est intéressant en ce qu'il rend manifeste à la fois la bonne volonté des directeurs et des futurs directeurs pour intégrer les impératifs de cybersécurité dans leurs pratiques professionnelles, et leur manque général de connaissances à la fois des sources de dangers et des cadres réglementaires dans lesquels s'inscrit la sécurité des SI.

Ainsi, à la question « En tant que directeur, vous sentez-vous concerné par la cybersécurité ? », la réponse est positive à 95%, et 75% des répondants disent « faire attention » au risque cyber avec les matériels informatiques professionnels. De même, l'idée d'exiger des garanties de sécurité de la part de prestataires SI est évidente pour 70% des répondants, mais 50% seulement retarderaient un projet pour des raisons de sécurité informatique.

Face à ces bonnes intentions, les pratiques semblent néanmoins plus fragiles : 55% des répondants disent ne pas éteindre leur ordinateur de bureau le soir, et 77% branchent des supports de stockage non validés par la DSI sur leurs appareils professionnels. La vulnérabilité due aux pratiques sont plus nettes encore en ce qui concerne la connaissance des réflexes en cas d'attaque : la marche à suivre est de se déconnecter rapidement du réseau en se mettant en « mode avion » ou en débranchant le câble Ethernet, avant même de contacter le support DSI. Or 10% seulement des répondants déclarent avoir ce réflexe, et 30% d'entre eux réagissent d'une manière inadaptée en ne faisant rien (5%) ou en forçant l'arrêt de la machine, ce qui compromet la recherche de

traces par les enquêteurs. La réponse « J'appelle la DSI » obtient 59% des réponses : cette réaction est caractéristique à la fois d'une volonté de bien faire, et d'une connaissance insuffisante des procédures d'urgence. En revanche, l'existence de l'ANSSI est connue par 80% des répondants, mais pas son rôle dans la gestion d'une attaque : l'agence est considérée comme le recours évident dans 59% des cas, mais c'est vers l'ARS que se tourneraient 38% des répondants, et 1% vers le Haut fonctionnaire de Défense et de Sécurité du SGMAS.

Les réponses concernant la protection des données et la connaissance du cadre réglementaire montrent que plus des trois quarts des répondants peuvent s'interroger sur la conformité d'un projet au RGPD (80%) et relient la cybersécurité à la protection des données (75%). Cependant, la connaissance concrète des acteurs du RGPD est assez faible : 48% des répondants sont en mesure d'identifier le RSSI et le DPO de leur établissement, 27% en identifient un des deux, et 25%, aucun. De façon similaire, l'autorité de référence de la sécurité des SI dans un établissement, son AQSSI, n'est connue que par 27% des répondants.

Les questions destinées à mesurer les connaissances informatiques étaient mal conçues et ne permettent pas aisément de mesurer le niveau des répondants : trop faciles et trop vagues, elles ne sont que difficilement exploitables. Ainsi, 95% des répondants savent qu'un antivirus ne protège pas de tous les virus, pas plus qu'un VPN. La question relative à la différence entre antivirus et *firewall*, en revanche, a été diversement comprise : 66% de répondants déclarent connaître la différence entre ces deux outils, mais on peut dès lors s'étonner d'un tel niveau de maîtrise technique comparé à une sensibilité médiocre à la question : la question portant sur le prochain grand sujet SI, tant à l'hôpital qu'en dehors, est l'objet d'un intérêt très faible : 63% des répondants n'ont pas d'opinion sur le déploiement de la 5G en santé alors même que la presse s'est fait l'écho de nombreux débats ; et pour les 36% de répondants ayant une opinion sur la question, la 5G en santé représente une « formidable opportunité » pour 23% et un « péril imminent » pour 14% d'entre eux.

B) Une faible capacité de projection

Une question ouverte, enfin, avait pour objectif de préciser quelle image les répondants se faisaient de la cybersécurité. Les réponses, libres, ont été analysées de manière à repérer quel aspect de la cybersécurité apparaissait comme le plus sensible. Les réponses sont les suivantes :

- Disponibilité : citée par 57% des répondants ;
- Confidentialité : par 55% ;
- Intégrité : par 5% ;

- Preuve / traçabilité : par 0%.

Comme on le constate, les problèmes liés à la disponibilité et la confidentialité sont, spontanément, les plus cités. Ils sont de fait, *a priori*, les plus « spectaculaires » dans leurs conséquences. Mais le fait que l'intégrité des données ne soient que si peu évoquées montre, sans doute, que le degré de maturité des répondants est encore assez faible. L'idée d'un *shutdown* général du SI apparaît donc comme le plus grand péril alors que des intrusions dans le SI peuvent prendre des formes beaucoup plus furtives et délétères par leur discrétion même. Quant aux problèmes de traçabilité, ils sont complètement oubliés alors que leur importance est majeure en ce qui concerne les médicaments ou la stérilisation.

Malgré ses maladresses et son faible nombre de répondants, ce sondage révèle donc certaines tendances intéressantes de la façon dont les futurs managers hospitaliers appréhendent la question de la sécurité des SI : sans grand intérêt, mais avec bonne volonté. Les grandes affaires très médiatiques de ces derniers mois ont à coup sûr contribué à renforcer un peu l'appropriation de ces enjeux, mais il reste, à l'évidence, des progrès à faire pour que la cybersécurité soit appréhendée par les futurs décideurs avec l'attention qu'elle mérite.

1.3 Conclusion

Le constat du manque de maturité des organisations hospitalières est généralement partagé par les spécialistes des Systèmes d'information. Prendre conscience de la réalité de la menace cyber et des principaux ressorts de son fonctionnement est une nécessité pour les managers hospitaliers, alors même que leur *habitus* professionnel et culturel ne les prédispose pas à tenir compte prioritairement de cet état de fait. Le milieu soignant n'est lui-même pas enclin spontanément à intégrer la cybersécurité comme une des facettes du soin. Par conséquent, un travail d'acculturation doit être mené pour responsabiliser et entraîner les personnels de l'hôpital.

2 MANAGER LA CYBERSECURITE

Une fois posé le constat de la difficulté d'intégrer la cybersécurité aux exigences du *management* hospitalier, il convient de s'interroger sur les outils dont dispose un directeur pour agir sur ses équipes et promouvoir une culture de la cybersécurité, mais aussi des procédures et des réflexes. Trois outils de natures différentes seront envisagés, dont le but est, in fine, la protection des patients à travers la sécurité de ses données. Le premier outil est celui de la réglementation (2.1), dont on proposera ici une synthèse. Le deuxième est celui de la formation (2.2), et le troisième, celui de l'intégration de procédures nouvelles, parmi lesquelles on compte la Cellule de crise hospitalière et le Plan de continuité de l'activité (2.3).

2.1 La réglementation de la cybersécurité

Le cadre réglementaire relatif à la sécurité informatique et à la protection des données commence à se stabiliser, et répond de plus en plus concrètement et clairement aux enjeux de la sécurité des systèmes d'information. Cette stabilisation était nécessaire du fait du retard de la législation sur les avancées techniques, retard qui, en 2010, pouvait justifier qu'on écrivît un article intitulé « Chroniques martiennes des données de santé numérisées : brèves observations sur une réglementation surréaliste »[37]. L'auteur y pointait l'incohérence entre l'incitation au partage de données d'un côté, et de l'autre, le renforcement de leur protection sans tenir compte de l'architecture même d'un système d'information. La réglementation récente de la sécurité informatique vient donc résoudre, sur le plan juridique, le conflit entre les contraintes de la préservation du secret professionnel et le fonctionnement du numérique en santé.

2.1.1 Cadre international

On peut rappeler que les Systèmes d'information sont l'objet d'une réglementation au niveau international, à travers la « Convention sur la cybercriminalité », ou **« Convention de Budapest"** » de 2001 du Conseil de l'Europe[38] . Ce texte est, d'après le résumé du Conseil de l'Europe,

> « le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques, traitant en particulier des infractions portant atteinte aux droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Il contient

[37] C. Zorn-Macrez, *Chroniques martiennes des données de santé numérisées : brèves observations sur une réglementation surréaliste,* RDS n°36, 2010, 331.

[38] Convention sur la cybercriminalité, STE n°185, Conseil de l'Europe, disponible sur https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008156d

également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception. Son principal objectif, énoncé dans le préambule, est de poursuivre "une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale ».[39]

Le **RGPD** de 2018 s'appuie en partie sur la Convention de Budapest, mais entre partiellement en conflit avec la législation extraterritoriale américaine du *Cloud Act* de 2018 dont il a été question plus haut.

2.1.2 Cadre national et européen

Ce cadre réglementaire est articulé en deux ensembles, le premier étant postérieur au second. Le premier est celui de l'obligation de moyens concernant la mise en sécurité technique des données personnelles, et en particulier des données de santé. Le second est l'obligation de résultat liée à la protection de ces données.

A) Lutter contre la fraude

Dès la fin des années 1980, la loi Godfrain (Loi n°88-19 du 5 janvier 1988) réprime la fraude informatique et les intrusions informatiques. Le législateur se désintéresse ensuite pendant une longue période du sujet, jusqu'aux années 2000, avec les textes relatifs au chiffrement[40]. Le volet concernant la mise en sécurité des systèmes d'informations commence, pour les Opérateurs d'Importance Vitale, par l'**Article 22 de la loi de programmation militaire** (loi n° 2013-1168 du 18 décembre 2013) : il concerne les Systèmes d'Information d'Importance Vitale des OIV.

La réglementation européenne fait évoluer cette première prise en compte du caractère spécifique de certains SI particulièrement sensibles avec la **Directive Network and Information System Security (NIS)** du 6 juillet 2016, inscrit en droit français par la loi de transposition du 27 février 2018 et par le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des Opérateurs de Services Essentiels, catégorie à laquelle appartiennent tous les CHU.

L'**Article L1110-4-1 du CSP** (LMNSS 2016 puis Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé) instaure la PGSSI-S afin de répondre aux obligations spécifiques des établissements de santé avec les « référentiels d'interopérabilité et de sécurité ».

[39] https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185
[40] Loi nº 2001-1062 du 15 novembre 2001, Loi relative à la sécurité quotidienne, art. 30 et art. 31 et Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : titre III, chapitre 1er, art. 29 à 40.

Cet arsenal juridique constitue la feuille de route que doivent suivre les DSI à court terme pour mettre en place des réseaux sécurisés aptes à garantir la sécurité des données de santé.

B) Protéger les données

La protection elle-même des données personnelles et informatiques est garantie par la **Loi du 6 janvier 1978, « Informatique et Libertés »,** qui a connu des évolutions et des précisions ces dernières années, et dont la dernière réforme d'importance est due au **Règlement Général sur la Protection des Données du 25 mai 2018.** Le droit européen vient donc consacrer un certain nombre de principes relatifs à la sécurité des données : sont établis les critères de transparence et de licéité, de limitation des finalités, de minimisation, de pertinence et de limitation dans le temps de leur conservation ; les droits des personnes physiques concernées sont garantis ; la sécurité des données, enfin, est mentionnée, à travers les différentes acceptions du terme : confidentialité, intégrité et disponibilité. C'est ce dernier aspect qui nous intéressera dans la présente étude, dans la mesure où cette question triple de la sécurité est au croisement des enjeux opérationnels d'un hôpital soumis à une attaque informatique.

La mise en œuvre de cette législation est pilotée par deux entités. Pour le premier volet, celui de la mise en sécurité des systèmes et les obligations en termes de sécurisations des systèmes d'information des OSE, c'est l'Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI, rattachée au SGDSN, qui est l'interlocuteur privilégié pour les actions de mise en conformité et les signalements en cas d'incident. Les agents de l'ANSSI sont amenés à se déplacer sur place lorsqu'une attaque de grande ampleur, du type de celle de Rouen, est perpétrée. La mise en œuvre des dispositions de la directive NIS et le contrôle reviennent à l'ANSSI.

Le deuxième volet que nous avons identifié, celui de la protection des données et de la mise en œuvre du RGPD, repose sur une agence beaucoup plus ancienne, la CNIL.

L'application spécifique de cette réglementation au secteur de la santé est pilotée, au titre de l'**Article L1110-4-1 du CSP** (Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé), par l'Agence du Numérique en Santé, qui déploie la Politique Générale de Sécurité des Systèmes d'Information-Santé, PGSSI-S, à travers l'application des « référentiels d'interopérabilité et de sécurité ».

C) La Politique de Sécurité des Systèmes d'Information

Au niveau de chaque établissement, enfin, doit être rédigé un document spécifique, la Politique de Sécurité des Systèmes d'Information. Ce document, qui s'appuie sur les

recommandations du Conseil de l'Europe du 25 juillet 2002, s'organise autour des neuf orientations suivantes[41] :

- Sensibilisation
- Responsabilité
- Réaction
- Éthique
- Démocratie
- Évaluation des risques
- Conception et mise en œuvre de la sécurité
- Gestion de la sécurité
- Réévaluation

Le PSSI constitue donc le document de référence au niveau local pour la mise en œuvre de la sécurité des données et des systèmes qui les stockent.

Au niveau de chaque établissement, le Directeur est l'Autorité Qualifiée en matière de Sécurité des Systèmes d'Informations, AQSSI, définie comme relevant des «autorités responsables de la SSI dans les administrations centrales et les services déconcentrés, ainsi que dans les établissements publics » et la « responsabilité ne peut pas se déléguer ». Son rôle est de :

- Définir une politique de sécurité des systèmes d'information adaptée à son organisme et en fixer les objectifs
- Assurer la responsabilité globale du niveau de sécurité requis
- Veiller à la mise en œuvre des dispositions réglementaires
- Procéder aux arbitrages et aux contrôles[42]

C'est donc l'AQSSI qui nomme le RSSI, son suppléant, et lui remet sa lettre de mission[43]. Le RSSI est donc en lien direct avec l'AQSSI en ce qui concerne les questions de SSI, mais aussi avec le HFDS des Ministères sociaux par l'intermédiaire du FSSI.

L'architecture réglementaire du contrôle et de la sécurité des données de santé peut être résumée par le schéma qu'on trouvera en annexe[44], et qui représente la structuration des textes et des acteurs de la protection des données au sens large. Ce document avait vocation à être présenté dans les différentes Commissions médicales d'établissements

[41] Memento PSSI de 2004 disponible à l'adresse : https://www.ssi.gouv.fr/uploads/IMG/pdf/pssi-memento-2004-03-03.pdf
[42] Eléments tirés de *L'instruction ministérielle relative à la protection des systèmes d'information sensibles*
n° 901/SGDSN/ANSSI NOR : PRMD1503279J, disponible sur
http://circulaires.legifrance.gouv.fr/pdf/2015/02/cir_39217.pdf
[43] https://services.renater.fr/ssi/securite/designation_des_rssi
[44] Voir Annexe 1

locales des HCL, ainsi qu'aux directeurs et responsables des fonctions supports et aux représentants des organisations syndicales. La crise sanitaire a reporté *sine die* ces présentations.

On peut noter l'assez grande complexité de cette architecture, en particulier à son sommet : la hiérarchie des normes ne va pas sans difficulté et la triple tutelle européenne, au titre des OSE, nationale-intérieur au titre de la protection des intérêts de la nation, et nationale-santé au titre du ministère de rattachement, impose aux responsables SI des procédures de déclaration souvent redondantes. Cette redondance se manifeste de manière particulièrement nette en ce qui concerne les signalements d'incidents. L'empilement des dispositifs (décret 2016-1214 du 12 septembre 2016, RGPD, et directive NIS de 2018) impose dans certains cas de contacter pour un même incident plusieurs interlocuteurs (Ministère, CNIL, victimes) selon des modes de déclaration différents[45].

D) Le cadre pénal

Pour finir sur les aspects réglementaires de cette question, on mentionnera certains des articles du Code Pénal réprimant les manquements aux obligations qui viennent d'être exposées. Sont par exemple punis de cinq ans d'emprisonnement et de 300 000 euros d'amende :

- « Art. 226-16 : le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi » ;
- « Art. 226-17 : le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites aux articles 24, 25, 30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 et aux articles 99 à 101 de la loi n° 78-17 du 6 janvier 1978 précitée » ;
- « Art. 226-17-1 : le fait pour un fournisseur de services de communications électroniques ou pour un responsable de traitement de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des articles 33 et 34 du règlement (UE) 2016/679 du 27 avril 2016 précité ou des dispositions du II de l'article 83 et de l'article 102 de la loi n° 78-17 du 6 janvier 1978 » ;
- « Art. 226-22 : le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de

[45] Cedric Cartau, « les cinq temps de la gestion des incidents SSI », *Ouvrage collectif SSI Santé*, Association pour la sécurité des SSI Santé, APSSIS, janvier 2019, page 85

traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ».

E) Les autres pertes

En plus des conséquences pénales pour les personnels des établissements de santé, une préparation insuffisante ou une prise en compte trop légère du risque cyber induit des risques financiers (rachat d'un parc entier d'ordinateurs, pertes de recettes) ainsi qu'une grave atteinte à l'image des institutions, dont les conséquences peuvent être durables. A cet égard, les chiffres concernant les déclarations d'incident de sécurité informatique, publiés en janvier 2020, sont éloquents : moins de 10% des établissements font des déclarations, ce qui ne reflète manifestement pas la réalité de la situation, et 90% des signalements sont faits pour des établissements publics, signe de la réticence des opérateurs privés à paraître vulnérables[46] alors que l'expérience récente de Ramsay Générale de Santé, en août 2019 (virus *Clop* déployé par le groupe *TA505*), montre que les structures privées ne sont pas à l'abri.

Pour toutes ces raisons, il semble que la prise en compte du risque cyber constitue un défi de taille pour les établissements de santé, et qu'il « est un risque à traiter au plus haut niveau de l'organisation et non plus seulement comme un risque dont l'évitement est l'affaire d'experts techniques »[47] selon les présidents de l'ANSSI, G. Poupard, et de l'AMRAE, B. Bouquot (Association pour le Management des Risques et de l'Assurance en Entreprise).

2.2 Développer une culture de la cybersécurité : promouvoir la montée en compétence

2.2.1 La formation au service de la cybersécurité : les fondamentaux

La sécurité informatique est aux HCL un enjeu déjà largement identifié et les mesures d'accompagnement et d'acculturation à la culture de la cybersécurité ont été prises depuis 2019 autour d'un support de formation continue fourni par la CAIH, Centrale d'Achat en Informatique Hospitalière.

[46] Géraldine Tribaul, « Les incidents de sécurité numérique restent sous-déclarés par les établissements », *Hospimedia*, Publié le 05/02/20, https://abonnes.hospimedia.fr/articles/20200205-systeme-d-information-les-incidents-de-securite-numerique/

[47] *Maîtrise du risque numérique : l'atout confiance*, Brigitte Bouquot (AMRAE), Guillaume Poupard (ANSSI), sans date de publication, https://www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/

La CAIH propose une solution e-learning développée par KTM Advance, filiale de l'éditeur de formation ITOP. Le marché, d'une durée de quatre ans, propose :

- « Une bibliothèque de ressources sur la sécurité des SI et la protection de données.
- Un portail de gestion des parcours et des utilisateurs.
- Un service de conception et de production de ressources propres ou personnalisées.
- Un service de conseil et d'accompagnement au déploiement de l'action de sensibilisation. »[48]

L'adhésion des HCL à ce marché permet l'accès à un support de formation comptant cinquante-et-une activités relevant du *serious game*, de la notice d'information ou du quizz, dans un format homogène de « capsules » indépendantes les unes des autres de moins de cinq minutes.

Ces activités sont organisées autour de six thématiques qui constituent un socle assez large de bonnes pratiques et de connaissances. Les thèmes abordés sont l'authentification, la sauvegarde des données, les questions de confidentialité, les usages mobiles, l'utilisation d'Internet et la bonne utilisation de la messagerie électronique.

Dans le cadre de mon étude, j'ai pu participer aux travaux menés conjointement par l'éditeur ITOP et l'OSSI des HCL, ainsi que les OSSI d'autres établissements pour le développement de nouvelles activités et l'amélioration de celles existant déjà. Ce travail est parti d'une étude du plan de formation déjà existant, et a consisté à repérer les éléments qui pouvaient manquer.

Il est apparu que les modules de formation déjà construits formaient un socle de bonnes pratiques principalement orienté vers la maîtrise technique de certaines opérations : la plupart des activités permettent de répondre à la question : comment utiliser le SI de façon sûre. Les différentes réponses orientent sur les thèmes relatifs aux mots de passes, aux particularités des terminaux mobiles, aux possibilités de sauvegarde des données.

2.2.2 Construction d'une formation cybersécurité à destination des personnels hospitaliers

Le groupe de travail a déterminé que certains axes manquaient à cette formation pour qu'elle puisse accompagner le plus grand nombre possible d'acteurs dans une prise de conscience plus approfondie des enjeux. Les nouveaux thèmes choisis et développés furent celui de la « *security by design* », du RGPD, de la sensibilisation aux enjeux et de

[48] Catalogue de la CAIH, page 31 sqq, consultable à l'adresse : https://caih-sante.org/wp-content/uploads/2020/03/Catalogue-CAIH.pdf

la maîtrise des procédures dégradées. On peut considérer que ces quatre nouveaux thèmes complètent de façon intéressante les précédents dans la mesure où ils ouvrent la réflexion de la cybersécurité à ses racines conjoncturelles (thème « sensibilisation »), structurelles (thème « *security by design* »), et à ses conséquences juridiques (thème « RGPD) et pratiques (thème « Que faire en cas d'attaque ? »).

Les sujets développés par le groupe de travail s'avèrent être particulièrement intéressants et porteurs, en même temps qu'ils sont des exemples éloquents des failles qui subsistent dans l'appréhension des enjeux de cybersécurité. Dans la mesure où les autres sont abordés au fil de mémoire, un seul de ces nouveaux thèmes sera développé ici : *Security by design*.

A) *Security by design* : un vœu plutôt qu'une réalité

L'inclusion du sujet *security by design* dans les modules de formation et de sensibilisation est fondamentale dans la mesure où elle marque une prise de recul dans la perception des enjeux de cybersécurité : considérée de manière globale, la cybersécurité commence avec la mise en place d'un outil connecté au réseau et se poursuit tout au long de l'exploitation de l'outil. Limiter la cybersécurité à un ensemble de bonnes pratiques est réducteur puisque les pratiques vertueuses sont insuffisantes si la structure de l'outil est elle-même vulnérable.

La sensibilisation à cet enjeu conduit également à rappeler aux décideurs - en l'occurrence, aux acheteurs et chefs de projet – que les caractéristiques de sécurité ne doivent pas être laissées de côté dans l'ensemble des critères présidant au choix d'un produit. La sécurité des outils disponibles sur le marché ne doit pas, en effet, être tenue pour acquise - au contraire, elle aurait plutôt tendance à avoir été systématiquement oubliée lors de la création des infrastructures globales des réseaux, et ensuite, des applications. Ce problème structurel est souligné sans fard par Guy Pujolle lorsqu'il dit que :

> « la sécurité d'Internet est un problème complexe pour la raison simple qu'elle n'a pas été introduite en même temps que les protocoles de départ. Pour arriver à vendre des produits rapidement, les équipementiers l'ont laissée de côté en pensant pouvoir l'ajouter facilement par la suite. En réalité, l'effort à faire pour ajouter les éléments de sécurité dans un réseau qui n'a pas été conçu pour cela pose de nombreux problèmes, dont les utilisateurs prennent conscience peu à peu. »[49]

[49] Guy Pujolle, *Les réseaux, 9ème édition, L'ère des réseaux cloud et de la 5G, 2018-2020*, Eyrolles, 2018, Paris.

En prenant cette fois le problème du point de vue de l'utilisateur, la *Revue stratégique de cyberdéfense* du SGDSN en 2018 évoque en des termes très nets les difficultés rencontrées :

> « Le recours à des produits et à des services de cybersécurité labellisés par l'ANSSI constitue un levier important pour assurer la sécurité des réseaux de l'Etat. Cependant, sa mise en œuvre se heurte à plusieurs obstacles, dont l'incompatibilité des cadres d'achat ministériels et interministériuels avec l'acquisition de telles solutions et l'insuffisance des budgets ministériels dans ce domaine. Par ailleurs, l'acquisition par l'Etat de solutions de sécurité est encore morcelée et, par conséquent, sous-optimale d'un point de vue économique »[50].

Certains éléments peuvent cependant guider objectivement dans le choix des solutions informatiques. Il existe des normes ISO/IEC concernant la sécurité des systèmes : ISO27001/270012 et ISO27034. Dans cette dernière, on trouve le schéma suivant, qui inscrit la sécurité informatique au cœur – et au début – du développement d'un logiciel :

Etapes du développement d'un logiciel applicatif[51].

Le respect de cette norme et son inclusion comme critère de choix – aux côtés d'autres certifications comme celle de l'ANSSI – devraient devenir systématiques. La démarche de certification aux normes 27xxx des établissements constitue en elle-même un projet lourd, onéreux, mais nécessaire.

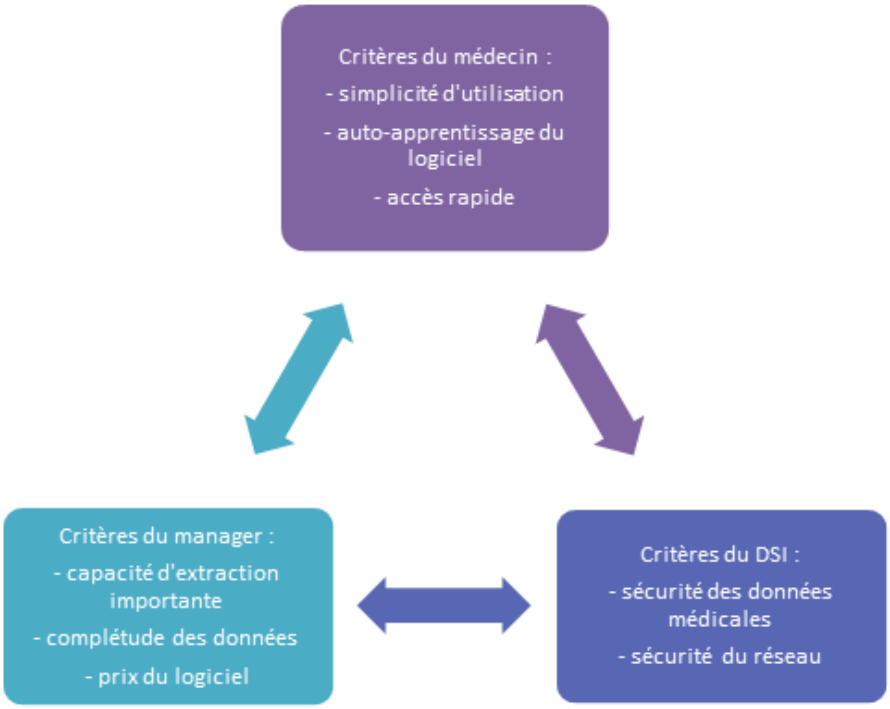
B) La question de l'équilibre : la sécurité en butte aux autres impératifs

En matière de cybersécurité, en effet, il faut, en dernière analyse, procéder à un exercice d'équilibre entre les trois extrémités du « triangle de la sécurité, de la fonctionnalité et du confort d'utilisation »[52]. Le renforcement de chacune de ces trois priorités concurrentes met en péril les deux autres, puisqu'une sécurité trop forte (étanchéité totale, identifications répétées, absence de cookies...) nuit à l'ergonomie et à la souplesse d'un outil, et sa simplicité de l'utilisation ne doit pas contribuer à en diminuer la performance ni

[50] Revue stratégique de cyberdéfense, 12 février 2018, SGDSN, page 58, disponible sur http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
[51] Schéma disponible sur https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27034:-1:ed-1:v1:cor:1:v1:en
[52] https://blog.infosanity.co.uk/?p=676

la sécurité. Selon l'utilisateur, chaque aspect sera présenté comme le plus important, à juste titre.

Pour ce qui est des logiciels-métier permettant, par exemple, l'enregistrement des actes médicaux, on pourra avoir à faire à une triple opposition de ce type :



Il est donc nécessaire de construire un dialogue entre les différents utilisateurs afin que chacun puisse exprimer quelles sont les limites qu'il ne peut franchir dans le domaine qui l'intéresse – une autre solution étant, pour le partisan de la sécurité renforcée, de permettre aux utilisateurs de participer à la sécurisation de l'outi. On trouve par exemple, dans une article de 2011, *Guidelines for Usable Cybersecurity : Past and Present*, deux propositions (parmi une vingtaine d'autres) de prise en compte des utilisateurs dans la sécurisation du système :

- « Rendre visibles et accessibles les fonctionalités de sécurité », car « cacher les fonctionalités de cybersécurité dans les paramètres avancés ou à des endroits séparés d'une interface risque de rendre la tâche de l'utilisateur plus difficile et, finalement, de nuire à l'ergonomie du système ».
- « Faciliter la création d'un représentation mentale fidèle » : il faut que l'utilisateur puisse se représenter mentalement la structure du système pour mieux appréhender les contraintes de sa sécurisation[53]

[53] Jason Nurse, Sadie Creese, Michael Goldsmith, Koen Lamberts, "*Guidelines for Usable Cybersecurity : Past and Present", Conference paper 2011*
https://www.researchgate.net/publication/224264159_Guidelines_for_usable_cybersecurity_Past_and_present/link/5524fb6e0cf2b123c517625f/download

L'idée qui sous-tend ces préconisations est que la sécurité du SI ne saurait être une matière *sui generis*, sur laquelle les utilisateurs n'ont aucune visibilité. Le fait de mêler au logiciel-métier des informations relatives à sa sécurisation aura plutôt tendance à susciter une participation active de l'utilisateur.

2.2.3 Didactique de l'appropriation des enjeux : pour une formation efficace

A l'image des campagnes portant sur d'autres sujets, de santé publique ou de sécurité routière par exemple, la démarche de sensibilisation au risque cyber, adaptée selon les caractéristiques du métier, mérite d'être réfléchie. Il apparaît de de façon assez nette, en effet, que la conscience de l'existence d'un risque ne garantit pas du tout que les mesures de sécurité vont être respectées – ou du moins, que tout le monde va, face à un risque identifié, adapter son comportement de façon à réduire ce risque.

A) Cybersécurité et homéostasie du risque

On peut reprendre à cet égard les analyses que Gerald J.S. Wilde a développées à partir de 1982, à propos de la sécurité routière, sous le nom de théorie de « l'homéostasie du risque »[54] ou de la « compensation du risque ». Cette théorie se fonde sur le postulat que la réduction du risque dépend uniquement du fait que les individus veulent réduire ce risque, et non composer avec les facteurs extérieurs permettant de le réduire. Consciemment ou non, chacun met en perspective le niveau de risque « cible » et le niveau de risque perçu. L'écart entre l'un et l'autre permet de décider s'il y a lieu d'adapter ou non son comportement. En définitive, les agents adaptent leur comportement aux modifications de l'environnement : dès lors, ils s'adaptent moins au risque lui-même qu'aux facteurs extérieurs permettant de réduire ce risque.

Résumée à grands traits, la théorie de l'homéostasie du risque, en matière de sécurité routière, revient à dire que la peur du gendarme et la ceinture de sécurité ont moins d'impact sur la traumatologie routière que la volonté de conduire prudemment. Dans certains cas, même, les sécurités extérieures introduites par la technologie (ceinture, airbags, plasticité du châssis...) conduisent à une augmentation du risque « cible », induite par la diminution du risque perçu. Cette théorie n'est pas unanimement acceptée, mais elle sert régulièrement à expliquer l'insuccès des campagnes contre le tabagisme.

[54] Gerald JS Wilde, "Risk Homeostasis Theory: An Overview" *Injury Prevention,* July 1998, consultable sur https://www.researchgate.net/publication/13619289_Risk_Homeostasis_Theory_An_Overview

B) Perception du risque et affects

Si l'on adapte ces réflexions à la cybersécurité, on peut tracer des parallèles qui peuvent éclairer, au moins en partie, le manque général de maturité en la matière. Dans un article de 2015, M. Bada, A. Sasse et J. Nurse écrivent :

> "Naturally, an individual that is faced with so many ambiguous warnings and complicated advice, may be tempted to abandon all efforts for protection, and not worry about any danger. Threatening or intimidating security messages are not particularly effective, especially because they increase stress to such extent that the individual may even be repulsed or deny the existence of the need for any security decision."[55]

Les auteurs introduisent d'autres notions, qui s'ajoutent à celles de l'homéostasie du risque : si le sentiment de sécurité est renforcé par des outils tels que les *antivirus*, le niveau acceptable de risque est, lui, défini de façon biaisée, soit qu'on sous-estime délibérément ce risque par pure incrédulité, soit qu'on n'ait pas les connaissances suffisantes pour comprendre l'existence même du risque. Dès lors, les campagnes de prévention à la cybersécurité risquent de manquer leur cible lorsqu'elles reposent sur la peur (un sombre *hacker* caché sous sa capuche devant un écran couvert de lignes de codes) ou sur des explications à la fois trop générales et contraignantes (en ce qui concerne la solidité des mots de passe par exemple).

En matière de cybersécurité comme de santé publique ou de sécurité routière, le postulat de la rationalité des agents n'est, de toute façon, jamais vérifié, et l'explication technique ne peut séduire qu'une frange marginale du public. Toutes les démarches de vulgarisation et de mise en application, y compris ludique, des concepts sont les bienvenues. On trouve une offre variée d'animations en lien avec la cybersécurité dans le domaine de la santé, selon différentes modalités, comme les journées dédiées et les *escape games*.[56] .Il incombe bien évidemment au Directeur de rendre possible, promouvoir et développer de telles initiatives.

2.3 Animer la montée et le maintien en compétence : s'exercer à des situations de crise cyber

Les actions de formation et de sensibilisation à la cybersécurité concernent l'ensemble des agents d'un établissement. Néanmoins, ces campagnes ne suffisent pas et il est indispensable (et obligatoire en ce qui concerne les OSE en vertu de la directive NIS) de

[55] Maria Bada, Angela M. Sasse et Jason R.C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", *International Conference on Cyber Security for Sustainable Society*, 2015, disponible sur https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

[56] Par exemple : https://www.esante-paysdelaloire.fr/fr/santescape/ et l'activité « Sant'Escape ».

les compléter, par des exercices plus ciblés au niveau de la direction générale et de la direction des soins. En ce qui concerne la direction générale, l'entraînement répété aux situations de crise cyber pourrait légitimement devenir une obligation, et pour la direction des soins, le travail sur les procédures dégradées dans les services de soin, en lien avec les fonctions logistiques, doit être mené pour étoffer les Plans de continuité de l'activité.

Cette partie pratique du travail de recherche a été initiée mais s'est interrompue du fait des circonstances sanitaires qui ont poussé au report d'un certain nombre de projets. Prévus pour être analysés dans le cadre de ce mémoire, les éléments présentés ici n'auront pas pu être testés ou développés dans le temps imparti.

Les outils étudiés sont l'exercice de cellule de crise hospitalière en cas d'attaque cyber, et la rédaction d'un Plan de continuité de l'activité en cas de crise cyber. Ces outils, à l'heure actuelle, sont en cours de construction dans la plupart des établissements sanitaires.

2.3.1 Construire un scénario de crise cyber

A) Les particularités de la crise cyber

La cellule de crise hospitalière, dans le cas d'une attaque, doit être réunie afin de prendre l'ensemble des décisions qui s'imposent. Cependant, ce type de crise n'a pas vocation à déclencher les procédures utilisées à l'occasion d'un incident sanitaire majeur. Une crise cyber obéit à une temporalité différente, et intègre d'autres acteurs que les crises sanitaires classiques. L'interdépendance totale des services d'un hôpital à travers son SI a pour conséquence qu'une telle crise a un impact nécessairement global sur l'organisation.

Les difficultés pour monter un exercice de crise cyber sont de trois ordres :

- L'absence de références en la matière et de fiches réflexes permettant de tester un dispositif : dans le cas présent, le dispositif reste à écrire.
- Le caractère transversal de l'incident, et le facteur de sa propagation : dans une crise cyber, les mesures prises en urgence ont des conséquences plus lourdes que l'incident lui-même. Ainsi, lorsqu'un cryptovirus est détecté sur un ensemble restreint de machines dans un secteur précis, le choix doit être fait de couper le réseau à l'échelle du site entier, voire de plusieurs sites. Après coup, il apparaîtra que la plupart des postes étaient sains. Par conséquent, toute intrusion dans le SI peut déclencher la mise à l'arrêt du réseau entier par précaution.
- Le caractère inadapté des équipements de sauvegarde et donc des procédures dégradées. Dans le cas d'une coupure accidentelle de l'accès au DPI, il est possible de travailler à partir des données des 24 dernières heures, récupérées sur un poste de sauvegarde quotidiennement mis à jour. Mais le fait que ce poste

ne soit pas isolé du réseau, dans la plupart des cas, entraîne sa contamination en cas d'attaque et son indisponibilité si le réseau est coupé par précaution. Théoriquement, le PC de sauvegarde devrait être un équipement dédié et isolé.

B) Cellule de crise hospitalière cyber

A partir de ces éléments, le choix a été fait de construire un scénario de crise cyber partant d'une attaque de *ransomware*, et de proposer un certain nombre d'injects destinés à tester la compréhension des enjeux cyber par les acteurs de la CCH, ainsi que leurs stratégies de communication. Un certain nombre d'autres sujets ont été mis de côté dans une proposition d'exercice se voulant être une introduction aux enjeux cyber plus qu'un entraînement à une procédure rodée. Ainsi, la question des télécommunications, qui peuvent être coupées dans le cadre de la coupure des réseaux, n'a pas été abordée. Elle nécessite en revanche d'être l'objet d'une réflexion menant, *a minima*, à la constitution d'annuaires papiers diffusés avec les numéros à dix chiffres.

Le scénario élaboré avec l'OSSI des HCL est le suivant : un vendredi soir, les écrans des postes de plusieurs services d'un site des HCL affichent un message annonçant que les données sont cryptées et qu'une rançon doit être payée. La Cellule de crise centrale est réunie et l'exercice commence. Le premier point à observer est celui de la décision de couper l'ensemble du réseau, même si seule une partie est infectée : l'enjeu d'empêcher toute contamination plus large, même si le remède semble pire que le mal.

Un certain nombre de péripéties surviennent ensuite, destinées à mettre les membres de la CCH face à différents choix tactiques, notamment en ce qui concerne la communication[57] :

- L'annonce de l'identification de l'attaque et de l'origine de la faille par la DSII
- La divulgation d'une rumeur selon laquelle des listes de patients circulent sur Internet,
- La mort d'un patient de réanimation dont le respirateur dysfonctionnait sans que le service s'en aperçoive du fait de la déconnexion du réseau et de la neutralisation des alarmes.
- Les demandes de renseignement émanant de collègues et des clients du logiciel *Easily* des HC

Ce scénario, inspiré des événements de Rouen et d'autres, a pour objectif de sensibiliser les acteurs de la Cellule de crise. Il porte uniquement sur les premières heures qui suivent le début de la crise. Les questions à régler sont donc prioritairement celles de la communication interne et externe, et de la compréhension de ce qui se joue avec un passage général en mode dégradé. Un aspect délicat est la nécessité d'informer sur la

[57] L'ensemble du scénario est consultable en annexe. 2

situation, sans divulguer d'éléments précis et techniques, et en tenant compte de l'inévitable diffusion sur les réseaux sociaux de nouvelles fausses et de conseils contre-productifs.

Les choix concernant la reprise d'activité sont volontairement laissés de côté car ils ne correspondent pas à l'urgence de ce moment particulier, et requièrent, en amont, une réflexion d'ensemble sur les délais exigibles de remise en service. Cette réflexion, encore à l'état embryonnaire, doit cependant être menée dans le cadre d'une stratégie de cybersécurité et sera présentée en troisième partie.

2.3.2 Faire l'état des lieux des procédures dégradées

L'état des lieux des procédures dégradées liées à un incident informatique de grande ampleur risque, dans un établissement de santé, d'être mené assez rapidement : les dispositifs d'urgence ou de crise, type Plan blanc, sont très aboutis, mais reposent en partie sur la fiabilité du Système d'information. Au fil des entretiens conduits aux HCL avec des personnels divers, il est apparu que l'indisponibilité durable du SI demeurait un impensé : de manière générale, on sait au niveau des directions que les procédures n'existent pas ou qu'elles sont peu fiables, et on suppose aux échelons inférieurs qu'elles existent.

En février 2020 a été mené dans deux unités un exercice de Plan de continuité de l'activité, conformément aux instructions de la Directive NIS, afin d'observer l'effet d'une coupure réseau de plusieurs heures dans des services de soin. Prévu pour se tenir un mardi matin, l'exercice a été annulé dans la mesure où une mise à jour du SI, survenue le vendredi soir, a déclenché une série d'erreurs qui ont rendu impossible l'accès au dossier patient pendant trois jours. Quelques jours avant, un agent de la DSII s'était déplacé dans le service pour s'assurer que les PC de sauvegarde étaient signalés comme tels et connus, et a pu constater que ce n'était pas le cas. Le volet « impression des prescriptions de sauvegarde » a donc pu être observé dans des conditions améliorées.

Le groupe de travail ayant conçu l'exercice a dès lors remplacé l'exercice prévu par la panne réelle, et travaillé sur le retour d'expérience de l'incident.

Les conclusions de ce Retex furent, entre autres, les suivantes :

- Des connaissances hétérogènes des procédures dégradées par les professionnels (selon l'audit qualité mené quelques semaines auparavant, le taux de connaissance déclarée de ces procédures, pour le Groupement Centre, s'élevait à 43%)
- La méconnaissance de la possibilité d'imprimer la pancarte dégradée
- Le caratère inutilisable de la prescription en mode dégradé : trop volumineuse, peu claire voire dangereuse car ne permet pas de distinguer facilement les

traitements suspendus ou repris, ni le rythme d'administration (ex : médicaments prescrits 1 jour sur 2).

- La multiplication de prescriptions orales
- La reprise du papier pour le relevé alimentaire
- La demande au laboratoire de rappeler le service n'a pas été entendue.

Le groupe de travail issu de la Direction des soins s'est attelé à travailler sur des modifications dans l'édition des bilans de prescription imprimés depuis le PC de sauvegarde.

De manière générale, le groupe de travail PCA a conclu a une très grande faiblesse des dispositifs existant, et a commencé à remédier aux manques les plus handicapants. Les autres exercices prévus n'ont pu se tenir du fait de la crise sanitaire.

2.4 Conclusion

Les enjeux de cybersécurité sont désormais encadrés de façon assez stricte par la loi. Le *manager* hospitalier est responsable de l'application de ce cadre juridique, mais il doit aussi veiller à ce que les personnels de l'établissement de santé s'acclimatent aux exigences de la sécurité informatique en développant une offre de formation adaptée à son public, et suffisamment bien conçue pour ne pas donner lieu à des pratiques non collaboratives. Au-delà des connaissances théoriques et pratiques en la matière, l'organisation d'exercice sur table ou grandeur nature est déterminante à la fois pour amener les agents à comprendre concrètement quels sont les risques de la menace cyber, et à repérer comment il est possible de s'en prémunir. L'animation des ces différents aspects ne peut reposer que sur le *top management* de l'hôpital, car il nécessite une participation active de tous les agents, quelle que soit leur fonction. L'intégration des médecins et des Cadres de santé, en particulier, est indispensable du fait de leur influence sur les équipes soignantes. La multiplicaité des interlocuteurs a pour conséquence le fait que la sécurité du SI ne saurait reposer uniquement sur les épaules du RSSI. Si celui-ci est un relai indispensable de la démarche décrite ici, il ne peut prétendre remplacer le directeur dans les choix stratégiques qu'il a à faire.

3 LE DIRECTEUR D'HOPITAL, STRATEGE DE LA CYBERSECURITE

Le Directeur d'hôpital, au-delà de son action tactique de remédiation face au risque cyber à travers la formation ou l'entraînement aux crises, doit également aborder la question de la cybersécurité de façon stratégique. L'approche stratégique est en effet purement du ressort de l'AQSSI. Les points qui seront abordés relèveront d'abord de la structuration du contrôle de la sécurité à travers la question de la place du RSSI, en partant du principe que le « responsable » à proprement parler n'est pas le RSSI mais l'AQSSI, et que le SI à proprement parler n'est pas un PC connecté (1). On verra enfin comment les sujets de l'achat et du budget hospitaliers sont des éléments essentiels de la sécurisation cyber des établissements (2).

3.1 Organiser le SI et son management : organigrammes RSSI

3.1.1 Interroger la place de l'informatique dans le système d'information et repenser le lien entre RSSI et DSI

La responsable de la sécurité des SI n'étant pas le RSSI mais le Chef d'établissement[58], il revient à ce dernier d'utiliser son pouvoir pour organiser la supervision des SI de la façon la plus efficace possible. Cette réflexion doit le conduire à considérer les SI pour ce qu'ils sont, et non comme un simple parc informatique connecté. Deux questions parallèles se posent à cet égard : celle de savoir si le SI est soluble dans l'informatique, et le RSSI dans la DSI. Cette prise de recul par rapport à la définition même des SI permet de conduire à une réflexion sur la cartographie des risques.

A) La vulnérabilité des systèmes connectés

a) La question du « tout réseau » : les SCADA et IoT

L'une des évolutions probables du développement des objets connectés, en dehors du domaine du biomédical, réside dans l'informatisation poussée de la Gestion Technique des Bâtiments, GTB, qui ne s'arrêterait pas au simple contrôle mais irait jusqu'à la prise-en-main à distance. Ces systèmes centralisés, voire automatisés, de contrôle existent et leur intégration au monde hospitalier mérite d'être réfléchie.

La notion de *built-in security*, en effet, ou « sécurité intégrée » ne semble pas encore être entrée entièrement dans les mœurs des constructeurs ni celle des acheteurs de systèmes techniques. Ce n'est qu'au gré des pannes et des accidents que s'est imposée l'idée qu'il était nécessaire de prévoir des dispositifs de secours primaire puis secondaire. En dehors

[58] Le RSSI des HCL a opté pour le titre d'OSSI, Officier de Sécurité des SI.

de la question de l'informatique, les HCL ont connu un incident dramatique en 1998 lorsque, à l'occasion d'une panne électrique, les groupes électrogènes ne se sont pas mis en marche[59]. Depuis, les procédures se sont largement étoffées, une mise en marche automatique et manuelle des groupes, des onduleurs et des circuits électriques redondants est déclenchée une fois par mois.

Cette *built-in security* « sur le tas », fruit d'empilement de procédures plutôt que d'une démarche consciente de management du risque, n'a pas accompagnée le développement de l'informatique comme cela aurait dû être le cas, pour des raisons économiques. La vulnérabilité des SCADA (*Supervisory Control And Data Acquisition*), systèmes de télégestion des équipements et des *process* dans le domaine industriel, est à cet égard inquiétante : en 2008, le virus *Stuxnet*, développé pour contaminer les installations industrielles iraniennes, s'est répandu jusqu'en Allemagne où il a compromis le logiciel SCADA *WinCC* de Siemens, tout en s'attaquant aussi aux centrifugeuses iraniennes. En 2015, un haut-fourneau allemand a également été mis à l'arrêt de loin grâce à une intrusion sur son SCADA. Les améliorations nécessairement apportées depuis aux systèmes employés dans l'industrie devront cependant à court terme s'adapter à la nouvelle technologie de la 5G qui démultiplie l'interconnexion des objets et des systèmes.

Dans ces conditions, et en considérant le manque de maturité globale des structures sanitaires françaises, l'une des questions que doit se poser le manager hospitalier est celle de l'opportunité de s'équiper de certains systèmes, tels que les SCADA, qui peuvent apporter *a priori* des avantages en termes de ressources humaines et de confort d'utilisation, mais constituent aussi une nouvelle source de vulnérabilité, et – ce qui est pire – de vulnérabilité mal connue.

Le rôle du Directeur d'hôpital en matière de cybersécurité doit aussi être celui du modérateur : de manière générale, on peut craindre qu'un établissement cherche à s'équiper de nouveaux systèmes dont les prolongements (comme les mises à jour et les maintenances) ne soient pas entièrement maîtrisés. Le contrôle d'opportunité dans le choix des équipements ne saurait donc se résumer à celui du coût d'une installation ou d'un nouveau logiciel. L'attrait pour la haute technologie ne doit pas aveugler la vision d'ensemble du manager hospitalier. Or cette question est appelée à se poser avec une fréquence de plus en plus élevée en raison de l'arrivée prochaine d'une nouvelle famille d'outils dont l'existence est rendue possible par l'amélioration technique des réseaux : il s'agit de la famille des objets connectés, désignés par l'expression *Internet of Things, IoT*, qui dépend de la mise en place du réseau de 5ème Génération, dit réseau 5G.

[59] https://www.lyoncapitale.fr/actualite/il-y-a-20-ans-edouard-herriot-responsable-mais-pas-coupable/

La forte augmentation des débits va permettre de connecter théoriquement tout appareil électrique au réseau afin de le faire bénéficier d'améliorations diverses. La question va donc se poser, à moyen terme, de savoir si l'on souhaite connecter au réseau tout un ensemble d'équipements biomédicaux dont les performances seront augmentées par la mise en réseau, mais dont la sécurité sera inévitablement mise en défaut. A l'heure actuelle, les expériences de prise de contrôle de voitures connectées, de caméras, d'enceintes connectées et même de pacemakers ont toutes été couronnées de succès.

La question de l'opportunité va donc se poser de façon déterminante, et il est indispensable que les *managers* de santé aient conscience des enjeux de sécurité de cette avancée technologique avant de s'y engager avec trop de confiance. L'une des principales fragilités de ces systèmes peut d'ores et déjà être pressentie : il s'agit de la possibilité de mise à jour des *softwares*. Sur une certaine période, proche de l'achat, on peut en effet postuler que la maintenance sera effective et efficace. Mais la prévisible obsolescence rapide de ces équipements entraînera soit leur maintien en fonction en dépit de l'arrêt des mises à jour de sécurité par le constructeur[60], soit leur remplacement par d'autres systèmes plus actuels, avec le risque de dépendance technologique que cela engendre.

b) Le Shadow IT

Parallèlement, le *manager* de santé doit aussi avoir conscience qu'une partie du réseau en fonction dans son établissement lui échappe : il s'agit là du domaine du *Shadow IT*, c'est-à-dire des équipements clandestins branchés sur le réseau par les utilisateurs, en toute bonne foi, mais sans considération de la portée potentielle de ces branchements sauvages. En théorie, aucun équipement personnel ne devrait être connecté à des équipements professionnels : cela vaut pour les dispositifs de stockage de type clef USB ou disque dur externe, mais aussi pour tous les dispositifs offerts ou prêtés par des constructeurs à des fins de test. S'il est nécessaire de les utiliser cependant, c'est au RSSI de les tester afin de s'assurer qu'ils ne sont pas infectés par un virus quelconque.

Les clefs USB peuvent en effet être un support particulièrement efficace d'intrusion du fait de leur banalité. On impute à cet égard aux services de renseignement russes la technique consistant à laisser trainer des clefs USB sur les parkings des ministères ou des entreprises : un agent la trouve, l'imagine égarée, et l'utilise par opportunisme. Généralement, la clef ne contient aucun document compromettant. En revanche, elle peut abriter un ver qui pénétrera discrètement sur la première machine à laquelle elle sera branchée. Dès lors, une première mise en sécurité du parc informatique consisterait à

[60] Voir par exemple https://www.healthcareinfosecurity.com/interviews/analysis-keeping-iot-devices-secure-i-4716

neutraliser tous les ports USB des ordinateurs de l'établissement, mais cette mesure n'est jamais prise pour des questions de coût. A l'occasion d'un stage au Centre de Traitement des Appels (CTA-CODIS) du SDIS du Rhône, j'ai pu en revanche constater que les terminaux utilisés au CTA étaient tous doublés : l'un était connecté à Internet pour les différentes opérations menées par les opérateurs, l'autre, lié à la seule téléphonie, était complètement séparé du réseau et ses ports USB étaient neutralisés[61].

Le *Shadow IT* peut prendre des formes beaucoup plus perfectionnées et difficiles à repérer. Une équipe de consultants *Orange CyberDefense* faisant l'audit d'un établissement de santé a ainsi pu repérer que le réseau interne avait fait l'objet d'une dérivation sauvage sur un routeur *WiFi* afin de permettre à des patients de se connecter à Internet[62]. Dans ce cas précis, c'est moins une quelconque volonté de nuire qui est à l'origine de cette faille de sécurité, que l'absence de conscience des risques qu'un tel détournement du système fait courir à la structure.

B) La place du RSSI par rapport à l'AQSSI

a) Le RSSI dans les EPS

Dans ce contexte, le rôle du Directeur d'hôpital ne peut en aucun cas être celui d'une instance de contrôle. En tant qu'autorité qualifiée pour la sécurité des systèmes d'information, AQSSI, le Directeur est tenu d'organiser les services de telle façon que les procédures de contrôle soient suivies. En dépit des termes, en effet, l'AQSSI est bien le responsable de la sécurité des SI, et sa responsabilité ne peut être déléguée, sans pour autant être RSSI. Mais c'est bien au RSSI qu'il incombe de vérifier la conformité du réseau à la réglementation, et d'intervenir lorsque des failles de sécurité sont repérées.

La première exigence est donc que les établissements de santé disposent d'un RSSI, ce qui est de plus en plus le cas. En 2018 cependant, 33% des GHT n'en disposaient pas encore[63], mais le rattrapage a été rapide depuis. Cependant, un doute peut subsister quant à la disponibilité d'un RSSI dont cette fonction précise ne serait qu'un aspect de sa fiche de poste. Car c'est bien souvent le cas dans des établissements de taille intermédiaire : le RSSI cumule sa fonction avec celle de *Data Protection Officer*, DPO, qui a remplacé le Correspondant Informatique et Liberté, CIL, et avec celle de directeur technique au sein d'une DSI. Or les enjeux de sécurité informatique impliquent que le métier de RSSI soit pleinement reconnu et que son pouvoir de contrôle soit garanti.

---

[61] Stage extérieur au Service Départemental Métropolitain d'Incendie et de Secours du Rhône, Lyon, septembre-octobre 2019.
[62] Entretien téléphonique avec Ludovic Jamart, *Orange Cyber Defense*, le 6 juillet 2020.
[63] Atlas des SIH 2018, Etat des lieux des systèmes d'information hospitaliers, DGOS, page 56, disponible sur https://www.atih.sante.fr/sites/default/files/public/content/3428/atlas_sih_2018.pdf

b) RSSI et DSI

C'est là que se pose une question de positionnement hiérarchique dans l'organigramme des établissements de santé, qui n'a pas encore été réglée de façon uniforme. Spontanément en effet, le RSSI a été intégré aux Directions des Systèmes d'Information, DSI, comme un élément parmi les autres de cette direction transversale. Cependant, ce lien de dépendance entre du RSSI envers la DSI pose *a priori* un problème de cohérence puisque le pouvoir de contrôle se retrouve subordonné à l'entité contrôlée. Si dans les faits le rapprochement entre RSSI et DSI se conçoit du fait de la proximité des activités de l'un et de l'autre, on peut considérer que le RSSI se retrouve à la fois juge et partie, et que son action peut se retrouver entravée par l'autorité du DSI. Par conséquent, les auteurs comme C. Cartau plaident pour que le RSSI soit rattaché au Secrétariat général ou à la Direction générale en tant qu'entité autonome de contrôle, et non à la DSI[64]. Ce positionnement extérieur à la DSI permet en effet, selon C. Cartau, de préserver l' « approche globale et non technicocentrée » qui doit être celle du RSSI, et de permettre davantage d' « aborder des questions touchant les processus des directions métiers sans qu'il y ait forcément des ordinateurs au sein du débat ». Malgré la confusion habituelle, le RSSI n'exerce pas son contrôle uniquement sur l'informatique, mais sur les systèmes d'information qui peuvent ne pas être informatiques. Dès lors, la question du contrôle d'opportunité dans le déploiement d'un nouvel outil lui revient, alors que son rattachement à la seule DSI informatique risque de le conduire à contrôler *a posteriori* les extensions du réseau.

En tant qu'AQSSI, le directeur a donc tout intérêt à donner au RSSI tous les moyens, y compris hiérarchiques, de mener à bien sa mission.

3.1.2 Cartographier les risques

A) Périmètre de l'impact d'un incident grave sur le réseau à l'hôpital : approche fonctionnelle

La connaissance fine d'un établissement de santé passe par une connaissance tout aussi fine de son système d'information. Le réseau du SI, en effet, se superpose à la cartographie physique d'un établissement, de telle façon qu'il est aussi nécessaire d'avoir à disposition les plans spatiaux du site que la carte des réseaux et des applications logicielles. Dans le cas des Opérateurs d'Importance Vitale, cette cartographie est

[64] Cédric Cartau, *op. cit*, page 72-74.

obligatoire[65], mais la cartographie du SI gagne à être employée dans tout établissement de santé, quelles que soient sa taille et la complexité de son infrastructure réseau[66].

Une première approche, thématique, permet de mesurer l'intrication des systèmes d'information et les conséquences d'une faille de sécurité.

a) Les infrastructures : fluides et courants.

En ce qui concerne l'alimentation en eau froide sanitaire et le circuit secondaire d'eau chaude, il existe un outil de GTC (Gestion Technique Centralisée), c'est-à-dire un système de supervision, et non de pilotage. Le choix a été fait de ne pas automatiser les pompes et vannes du réseau, et de maintenir des équipes de maintenance *in situ* qui sont à même d'agir sur le réseau manuellement.

L'électricité (courants faibles) obéit aux normes de sécurité lourdes liées aux activités de dernier recours de l'hôpital. Les réseaux d'alimentation électrique sont connectés par un système d'information autonome, notamment en ce qui concerne les groupes électrogènes et les onduleurs des blocs opératoires. D'après le responsable des courants faibles m'ayant présenté les installations, « le meilleur antivirus est de ne pas être sur Internet »[67], (ce qui n'est pas nécessairement vrai).

b) Les bâtiments

Aux HCL, l'accès aux bâtiments est permis ou empêché par un système de badges à bande magnétique chargée selon les habilitations du titulaire : accès aux bâtiments, aux zones réservées, aux zones critiques et hyper-sécurisées. Il existe six catégories de locaux, associées à des profils professionnels particuliers et désignés par des couleurs. L'ensemble des accès internes et externes de tous les sites est contrôlé à distance, et l'état des ouvertures (ouverture / ouverture anormale-porte bloquée / fermeture) est référencé en temps réel. Ce système de contrôle est connecté au réseau, ce qui permet une supervision globale de l'ensemble des sites, étage par étage, avec indication des anomalies graves : ouverture anormalement longue de portes donnant accès à des locaux sensibles. Le système de supervision permet également de fermer à distance certains secteurs.

c) Les communications téléphoniques

[65] Au titre de l'annexe I des arrêtés sectoriels fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale pris en application des articles R. 1332-411, 2 et 13 du Code de la Défense.

[66] *Cartographie du système d'information, Guide d'élaboration en cinq étapes,* ANSSI, novembre 2018.

[67] Entretien avec le responsable des affaires techniques en charge des courants faibles, 05/03/2020.

Le troisième sujet est celui de la téléphonie et des DECT. Connectés au réseau, les téléphones fixes ne sont plus utilisables en cas de panne informatique. Seuls continuent à fonctionner les DECT (*Digital Enhanced Cordless Telecommunications*), avec la nuance suivante : les numéros à six chiffres ne sont plus opérationnels, il faut reconstituer les numéros complets à dix chiffres. Retrouver l'indicatif propre au site ne pose généralement pas de problème. En revanche, les annuaires ne sont plus accessibles. Par conséquent, seuls quelques numéros enregistrés sur les appareils peuvent être joints.

La question des communications téléphoniques et de la résilience des réseaux de téléphone n'a pas encore été véritablement investie. Si des incidents ont pu survenir, l'absence de conséquences graves a probablement empêché que le sujet soit sérieusement traité. C'est le constat fait en 2018 dans la revue *Techniques hospitalières* à propos d'une coupure des réseaux téléphoniques survenue à l'Hôpital d'Instruction des Armées Bégin en septembre 2018 : « Le risque [lié à la téléphonie,] encore mal maîtrisé par les établissements de santé, fait plutôt l'objet d'une gestion *a posteriori*. Peu d'éléments sont retrouvés dans la littérature »[68].

d) Les équipements biomédicaux

Les équipements biomédicaux font partie des outils qui sont, dans les prochaines années, les plus susceptibles d'évoluer vers une mise en réseau du fait du déploiement de la 5G, réseau *WiFi* de 5ème génération : cette évolution de la technique de transmission sans-fil va rendre possible une multiplication radicale du nombre d'objets connectés.

Le progrès engendré par ces outils connectés sera vanté à juste titre pour les gains en précision, en rapidité etc qu'ils procureront. On peut citer les pompes à morphine connectées, les pousse-seringue, les scanners ou encore les couveuses. A l'heure actuelle, ces équipements sont généralement indépendants du réseau, et les données qu'ils génèrent doivent être l'objet d'un retraitement pour être intégrées au DPI. Le projet d'interconnecter DPI et équipements biomédicaux représente donc, *a priori*, une occasion de sécuriser les transmissions entre les différentes briques SI. L'inconvénient réside dans le manque avéré de sécurité de ces équipements, qui peuvent devenir des portes d'entrée dans le reste du réseau, mais aussi être l'objet d'attaques visant à toucher l'intégrité des données : il est techniquement possible de modifier la programmation d'un respirateur ou d'une pompe à morphine à distance si l'on s'introduit dans le SI et que l'on gagne les accès nécessaires. En juin 2020, les autorités de contrôle américaines ont ainsi rendu publiques les failles concernant six équipements connectés de dialyse, de perfusion ou des *pacemakers*. Les compromissions peuvent soit entraîner une modification des

[68] Stéphane Demaison et alii, « Panne de téléphonie : gestion de crise, retour d'expérience à l'hôpital Bégin », *Techniques hospitalières*, mars-avril 2019, p. 775.

paramètres de fonctionnement des équipements, soit l'utilisation des équipements comme réseau de *BotNet* destinés à alimenter une attaque *DoS*[69].

Cette compromission possible des équipements biomédicaux doit conduire *a minima* à s'interroger sur le déploiement de cette technologie, et à mettre en œuvre une politique de sécurité stricte. En ce qui concerne les appareils d'imagerie, le constat général est que les logiciels d'exploitation sont en général mal protégés, du fait par exemple du maintien de mots de passe par défaut. Imaginer un parc décuplé d'équipements connectés a de quoi susciter des inquiétudes chez l'AQSSI d'un établissement de santé.

Les éditeurs d'antivirus attirent d'ores et déjà l'attention sur les risques actuels et les tendances futures qui vont toucher les équipements biomédicaux connectés. Cette sollicitude laisse augurer un risque de dépendance technologique croissant à l'égard des fournisseurs d'équipements biomédicaux, de la maintenance logicielle de qui dépendra une bonne partie de la sécurisation, et des éditeurs d'antivirus ou de solutions de détection d'intrusion, qui peuvent envisager un développement exponentiel du nombre d'objets à sécuriser. Le document de *TrendMicro*, reproduit en annexe[70] synthétise ces enjeux : il rappelle notamment l'impact du virus *Wannacry* de 2017 sur les équipements biomédicaux des hôpitaux britanniques, et le mouvement permanent vers une plus grande intégration au SI des outils afin de collecter plus de données.

e) Les logiciels

Les logiciels-métiers sont un point central de l'activité de soin et des fonctions supports. Ces logiciels sont utilisés en permanence et sont devenus indispensables pour la réalisation de l'ensemble des gestes. La cartographie de l'ANAP permet de se représenter le nombre de logiciels différents utilisés et correspondant les uns avec les autres. La sécurité de ces logiciels, qui correspondent à la couche sémantique du système, est assurée du point de vue de l'utilisateur par les identifiants. Un agent pouvant avoir accès à un grand nombre de logiciels, il est indispensable de tenir à jour la liste des identifiants et des privilèges associés à chaque compte. Ce référencement relève de la gestion de l'*Active directory* et de l'établissement d'un FICOM solide.

Au niveau logique, la sécurité des logiciels dépend de plusieurs facteurs, en particulier de leur système d'exploitation (OS), dans la mesure où tous les systèmes ne courent pas les mêmes risques. Un virus peut en effet infecter un système d'exploitation, mais laisser intacts les autres. De manière générale, les logiciels sous Windows courent plus de

[69] Marianne Kolbasuk McGee, "Alerts: Vulnerabilities in 6 Medical Devices : DHS Warns of Security Issues in Devices from Baxter, BD and Biotronik", *HealthCare InfoSecurity,* 19 juin 2020 https://www.healthcareinfosecurity.com/alerts-vulnerabilities-in-6-medical-devices-a-14476

[70] https://www.dsih.fr/images/InfographiesanteTrendMicro14062019.pdf
Cf Annexe 4

risques d'être l'objet d'attaques que ceux exploités par Linux ou Mac/OS du fait de leur plus grande diffusion, et donc de la plus grande « rentabilité » d'un virus les visant. Ainsi, lors de l'attaque de Rouen, tous les logiciels sous Windows ont été bloqués par le *Ransomware*, les autres sont restés indemnes. Aux HCL, comme dans la plupart des établissements, les logiciels dépendant de Windows constituent 80% du parc, les 20% restants sont exploités par différentes versions d'UNIX.

Concernant les logiciels, l'une des questions majeures concerne le délai exigible de remise en service après une coupure, sachant que le degré de criticité de certains est largement inférieur à celui d'autres outils. Lors de la phase de reprise d'activité, un choix doit donc être fait pour orienter le travail des techniciens, ce qui implique qu'un ordre de remise en service ait été préalablement établi. Les conflits de priorité ne manquent pas de survenir à cette occasion, et il est indispensable d'avoir réfléchi à la question en prévision de la coupure.

f) Les cartes professionnelles

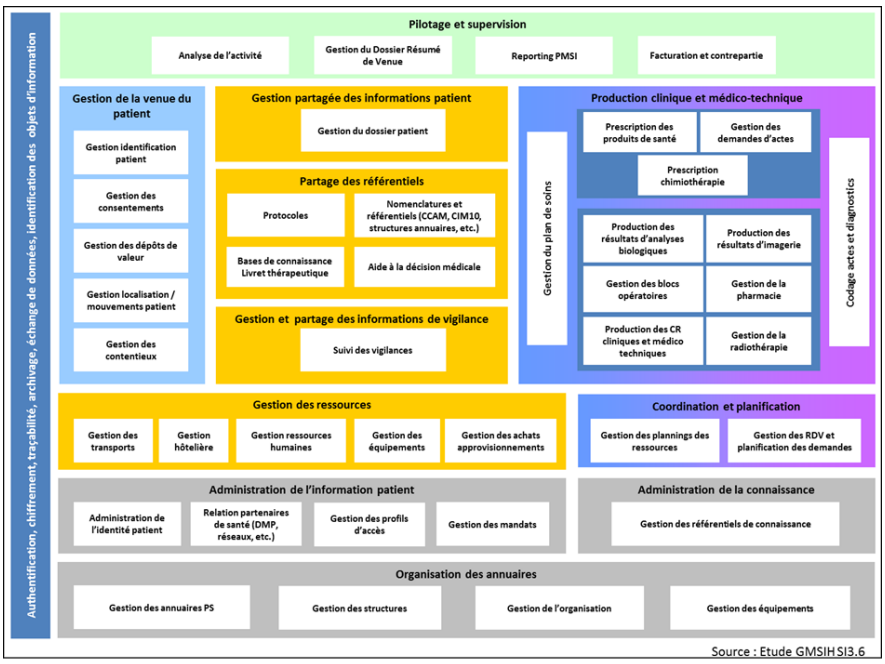
La question de la Carte Professionnelle de Santé se pose à tous les niveaux de l'architecture d'un hôpital, depuis le *hardware* bâtimentaire jusqu'aux *softwares* logiciels. Liée au domaine de la cryptographie, la CPX (les différentes variétés de cartes professionnelles) constitue un enjeu financier et organisationnel de premier plan puisque l'infrastructure générale du système d'information est parallèle à celle de la CPX.

A l'heure actuelle, environ 360 000 cartes valides sont comptabilisées par l'ANS[71] dans le milieu hospitalier, soit 30% des effectifs. Les quatre critères de la cybersécurité du DICP ont pourtant partie étroitement liée avec le déploiement de la CPX : la systématisation de ce système de gestion des identifiants (*Identity Access Management*, IAM) serait donc souhaitable.

B) L'approche réglementaire de la gestion des risques selon la méthode HOP'EN

Une autre approche, plus conforme aux exigences de cartographie de la législation, mais aussi plus complexe à mener, consiste à partir des briques logiques du SIH telles qu'elles sont modélisées par l'ANAP :

[71] Site de l'ANS . Document misà jour le 4 juin 2020. https://esante.gouv.fr/sites/default/files/media_entity/documents/Tableau%20de%20suivi%20des%20cartes%20valides_2020-06-04-15-05-05.pdf



A chacune de ces briques, il est possible d'associer un ou plusieurs logiciels métiers, et d'établir entre tous ces logiciels les liens représentant leur connexion à un même réseau. Cet effort, tel qu'il est demandé par un outil comme EBIOS[72] (ANSSI), impose également de s'interroger sur la criticité de chaque brique et son délai supportable de remise en service. Si certaines briques, en effet, peuvent rester inertes pendant plusieurs jours ou plusieurs heures, d'autres exigent une disponibilité permanente, de l'ordre de 99, 999% (soit 5 minutes d'indisponibilité par an). Le travail de modélisation demandé par cette méthode est de très grande ampleur puisqu'il requiert de demander aux utilisateurs de décrire précisément leur usage des outils du SI et leur « degré de dépendance ». C'est de la réalisation de cette cartographie que peut naître un Plan de Continuité de l'Activité, en particulier en ce qui concerne les délais de remise en route.

Dans le cadre de la démarche de certification « Qualité Hôpital Numérique », l'ANAP met à disposition une boîte à outils[73] dont trois chapitres en particulier permettent de cartographier les risques :

- la fiche 3 : PRA et fonctionnement en mode dégradé
- La fiche 4 : évaluation des taux de disponibilité
- La fiche 8 : cartographie applicative.

Suivre les préconisations de ces trois fiches impose de constituer des groupes de travail animés par un chef de projet déterminé vu la densité et la complexité de la matière.

[72] https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
[73] *Atteindre les prérequis HOP'EN, Boîte à outils*, ANAP, juin 2019

3.2 Diriger les évolutions et les prévoir : achat et budget

3.2.1 Intégrer la cybersécurité aux achats

La *Revue stratégique de cyberdéfense* de 2018 met l'accent sur le sujet particulier de l'achat public :

> « La revue recommande d'élaborer des clauses contractuelles types regroupant les bonnes pratiques de sécurité applicables dans l'acquisition d'une solution informatique et d'inciter fortement les ministères à systématiser l'inclusion de ces clauses dans leurs marchés publics comprtant un volet numértique »[74].

En l'absence de réflexion sur l'acquisition de matériels ou de solutions vulnérables, en dépit des facilités d'emploi ou de la qualité des interfaces, les bonnes pratiques de sécurité ne suffisent pas à protéger un Système d'information, et des coûts supplémentaires risquent finalement de conduire à payer plusieurs fois le prix du produit : la maintenance des systèmes, les mises à niveau de sécurité, l'adjonction de *patchs* correctifs et la nécessité de réparer des failles qui n'avaient pas été perçues ou anticipées, sont génératrices de surcoûts importants dont il doit être tenu compte lors de la passation d'un marché. La difficulté qui se présente est réelle :

- Les acheteurs n'ont pas nécessairement les compétences pour évaluer le niveau de sécurité embarquée de l'outil ;
- Le RSSI n'a pas nécessairement les moyens de contrôler en toute connaissance de cause la sécurité de l'outil ;
- Les utilisateurs finaux ont une voix déterminante et peuvent avoir tendance à privilégier l'ergonomie et le confort d'utilisation à la sécurité.

En définitive, les déclarations du vendeur risquent d'être le seul élément de réflexion à disposition des acheteurs.

On peut donc partir du principe que la sécurisation de l'ensemble du réseau passera par une prise en compte systématique par les acheteurs hospitaliers de cet enjeu, et de l'inscription de clauses particulières dans le règlement de la consultation, dans le CCAP et dans le CCTP. L'inscription de ces clauses doit permettre aux établissements de santé

- de s'assurer de certaines restrictions concernant le recours à la sous-traitance de la part du titualaire,
- de se prémunir contre l'obsolescence des équipements en s'assurant de la portabilité des données, de leur réversibilité et de leur transférabilité,

[74] *Revue stratégique de cyberdéfense*, 12 février 2018, SGDSN, page 59, disponible sur http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

- d'avoir connaissance des incidents de sécurité touchant le SI du titulaire du contrat,
- d'avoir l'assurance que les données de l'acheteur, si elles sont hébergées chez le titulaire, ne peuvent être au contact d'autres données d'autres acheteurs,
- de s'assurer que le titulaire dispose lui-même d'un Plan de continuité de l'activité.

Ces éléments sont tirés d'un document de travail en cours d'élaboration par l'ANSSI et la Direction des Achats de l'Etat, le *Guide de clauses de sécurité à intégrer dans les marchés publics*[75]. La « méthode » préconisée par le guide constituera une base indispensable pour la passation de marchés publics intégrant des SI, qu'il s'agisse de prestations intellectuelles, d'hébergement, d'exploitation et de supervision, de recherche ou d'achat de matériels et de logiciels. Concrètement, il s'agit donc d'intégrer RSSI et DPO à la fonction achat.

3.2.2 Repenser les budgets SI

La question du financement de la cybersécurité, enfin, constitue un élément déterminant de la stratégie des directeurs. Dans le cadre contraint du financement des établissements de santé, les DSI constituent un service purement dépensier, sur le plan comptable, et leur financement peut, dans un grand nombre de cas, constituer une variable discrète pour soutenir le cœur d'activité soignant. De fait, le budget des SI s'élevait en 2015 en moyenne à 2%[76], en 2020 à 1,6%, chiffres qu'on peut mettre en relation, *mutatis mutandis*, avec les 10% que représentent les SI dans le secteur bancaire. L'écart est frappant, en particulier si l'on considère que les données de santé ont une valeur marchande plus élevée que les données bancaires, en partie en raison de leur durée de vie plus longue (les conséquences du piratage d'un compte bancaire sont immédiatement visibles, alors que celles d'une carte Vitale peuvent passer inaperçues). Mais la comparaison n'est pas entièrement pertinente si l'on considère qu'une banque se résume à son SI, ce qui n'est pas le cas d'un hôpital.

A) Le financement de la cybersécurité

Aux HCL, le budget de la DSI (en classe 2) s'élève à 22M€, soit 1,2% du budget total. Ce chiffre exclut le budget du GIE Hopsis qui développe le logiciel *Easily* ainsi que les travaux d'investissement dans le réseau MAN, inscrits aux budgets G du GHT. Au sein de ce budget, la part qui revient à la sécurité représente 2%, soit 500K€ gérés par l'OSSI. Ce budget fléché se divise lui-même en un volet « sécurité opérationnelle », pour 60%, qui

[75] https://democracyos.consultation.etalab.gouv.fr/guideclausessi/topic/5d0b79c5e486af05eff949c5
[76] TICSanté, 22 mai 2015, https://www.ticsante.com/story/2403/les-systemes-d-information-representent-en-moyenne-2-des-depenses-des-etablissements-de-sante-(atlas-des-sih).html

regroupe le financement d'outils tels que l'*Endpoint Detection and Response* (EDR[77], sous-traité), les PKI, les logiciels de protection périphérique, de concentration et corrélation de traces. Les antivirus eux-mêmes, en revanche, sont à la charge de la Direction technique de la DSI. Les 40% restant sont consacrés aux fonctions d'audit et de maîtrise d'œuvre en sécurité. La sécurité va donc au-delà du seul budget fléché, puisque l'hébergement des données, par exemple, qui est isolé sur le plan comptable, inclut 20% de financement au titre de la sécurité.

Les entretiens menés auprès de différents acteurs des SI n'ont pas fait unanimement ressortir le constat de sous-financement des SS en général et de la cybersécurité en particulier. Pour certains, les ressources financières étaient satisfaisantes, mais le manque venait plutôt du nombre insuffisant d'agents en mesure de mener des projets ou de procéder à l'analyse de risques. Pour d'autres, l'insuffisance des budgets SI est considérée comme structurelle et dangereuse.

B) Financements internes et externes

Le reproche traditionnel de sous dotation des DSI, et donc de la cybersécurité, ne se pose cependant pas de la même manière dans un grand CHU comme les HCL et une petite structure. Les économies d'échelle font qu'un établissement de petite taille, à budget relatif équivalent, peut avoir des difficultés beaucoup plus grandes à financer, par exemple, un RSSI à temps complet. A cet égard, les GHT constituent une opportunité pour les petits établissements - en plus du fait que la nature même du domaine des SI, en réseau, appelle nécessairement une gestion décloisonnée et holistique du système : les RSSI sont, de fait, nommés au niveau du GHT.

La prise en charge de la sécurité doit donc nécessairement, dans l'état actuel du financement des hôpitaux, passer par le recours à des ressources extérieures au budget propre : il existe des financements possibles de la part des ARS sur la base d'appels à projets. Le directeur a un rôle éminent à jouer dans la promotion et le choix des projets à financer, en fonction de la situation de son établissement.

De façon corollaire, on peut supposer que la maîtrise du risque informatique va intéresser de plus en plus les assureurs, qui prévoient d'ores et déjà de moduler le montant des primes en fonction de la maturité de leur client en termes de gestion des risques. Anticipant une inscription de critères de cybersécurité retenus par la HAS (au titre du plan Hôpital Numérique) dans les programmes de financement à la qualité, un assureur

[77] L'EDR est un outil d'analyse comportementale destiné à repérer des mouvements suspects, caractéristiques d'un virus, dont le code inconnu ne peut être détecter par un antivirus. Source : https://orangecyberdefense.com/fr/solutions/protection-des-mobiles-et-des-endpoints/endpoint-detection-and-response-pourquoi-ledr/

comme la SHAM[78] commence à s'intéresser à la façon dont les établissements vont faire face à la multiplication des équipements biomédicaux connectés. Aux yeux de l'assureur, la question de la sinistralité liée aux équipements biomédicaux connectés est d'ores et déjà considérée comme une réalité. L'analyse de risque mettant en avant une prise en compte solide de la cybersécurité pourra entraîner l'attribution de bonus sur les montants des primes.

C) Perspectives : un autre financement / un autre Internet

a) Security as a service *?*

L'enjeu stratégique de la cybersécurité est de la considérer non plus comme un coût, mais un élément central de la gestion des risques, voire une action qualité. On pourrait dès lors envisager une modification de son système de financement selon une approche renouvelée de comptabilité analytique s'appuyant sur le modèle *Activity-Based Costing*, ABC, qui partirait de l'idée d'une « consommation » de cybersécurité par l'ensemble des services « clients ». L'objectif serait de responsabiliser l'ensemble des utilisateurs en modélisant une consommation de cybersécurité conçue à partir, par exemple, du nombre d'agents formés, des résultats des tests de *phishing*, et d'une évaluation du respect des bonnes pratiques réalisée à partir d'audits. Dans le cadre de la construction des CRéA, une partie des coûts indirects de la cybersécurité se transformerait en coûts discrétionnaires. Ainsi, les services « clients » de la DSI seraient en mesure de faire baisser leurs CréA, et la méthode employée, qui repose sur l'appropriation des règles d'hygiène informatique, contribuerait à une baisse de la sinistralité informatique (en partant du principe que les erreurs commises par les agents sont à la base d'une grande partie des failles dans les Systèmes d'information).

b) Le coût de la sécurité

Une telle méthode de comptabilité analytique nécessiterait cependant une plus grande maturité des organisations. C'est peut-être l'évolution du fonctionnement même des réseaux qui va la rendre inévitable : jusqu'à maintenant, Internet a fonctionné d'une façon toujours plus décentralisée, multipliant les serveurs physiques et les redondances. Ce système garantissait sa fiabilité et sa disponibilité en permettant un routage multiple des données. Mais il repose également sur une consommation électrique exponentielle, qui va être l'objet d'une contestation de plus en plus vive dans les années – voire les mois – à venir, et d'autant plus que l'arrivée de nouveaux objets connectés va la faire exploser. On peut considérer théoriquement qu'à budget constant, les dépenses en fonctionnement

[78] Entretien avec E. Trividic, Directeur des Partenariats et des Relations extérieures de la SHAM, Lyon, 16 juillet 2020.

vont augmenter rapidement, pesant mécaniquement sur le financement de la sécurité. Il est inévitable, donc, de chercher à optimiser les coûts de la cybersécurité qui, d'après C. Cartau, « coûte cher et va coûter de plus en plus cher »[79].

c) Green IT *et économies de fonctionnement*

Une autre approche des transformations probables est possible si l'on considère que 10% des émissions mondiales de GES sont dues à Internet, en raison de son architecture : il semble inévitable de reconsidérer ce mode de fonctionnement et de reconstruire un réseau beaucoup plus centralisé, en s'appuyant notamment sur le *Software Defined Networking*, SDN : le principe en est que les machines physiques vont être remplacées par des machines virtuelles contenues dans le *cloud*. Un serveur physique pourra donc contenir un nombre de machines virtuelles évolutif, en fonction de la demande et du besoin. Le phénomène de virtualisation des serveurs est cependant déjà en œuvre dans nombre de structures hospitalières, et les gains possibles s'amenuisent au fur et à mesure de la conversion des serveurs physiques (qui a, par exemple, représenté pour les hôpitaux du Centre un gain de 1,9M€[80]) La question reste posée, cependant, de la perspective d'une augmentation radicale du nombre d'objets connectés, de leur alimentation en courant électrique et en données, et de leur sécurisation. Que ce soit pour les hôpitaux ou les particuliers, il n'existe à l'heure actuelle aucune réponse satisfaisante à ces défis.

Appliquée au SI hospitalier, une architecture hébergée essentiellement sur un *cloud* posera des défis de sécurité particuliers qui rendront caduque une partie des constats faits dans ce mémoire. Un tel mouvement d'externalisation du stockage des données et des logiciels entraînera nécessairement la possibilité d'une externalisation complète de la gestion du SI, ce qui n'ira pas sans poser de nouvelles questions de financement et de responsabilité.

d) *Un SI de GHT intégré : une stratégie complexe.*

L'intégration des SI au sein des GHT, constituerait un réel changement de paradigme managérial : la question du financement d'en trouverait posée dans des termes nouveaux, ainsi que celle de la définition même du réseau des SIH. L'intérêt de la connexion du SI à Internet est, justement, de permettre la mise en réseau de plusieurs SI, et non de les juxtaposer. Un SI commun à un GHT serait donc possible et souhaitable, une fois tous les *process* internes identifiés et cartographiés – ce qui est loin d'être le cas à l'heure

[79] Cédric Cartau, *op. cit.*, page 267.
[80] AProgramme ARMEN, phase 2, *Base de donnée des bonnes pratiques Armen*, https://solidarites-sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante-medico-social/performance-des-etablissements-de-sante/phare-11061/armen-et-les-echanges-de-bonnes-pratiques/article/la-base-de-donnees-des-bonnes-pratiques-armen

actuelle : en ce qui concerne les RH, un SI de GHT ne peut entrer en fonction qu'une fois harmonisées les pratiques locales concernant par exemple les RTT. Au niveau médical, un logiciel de prise de rendez-vous informatisé imposerait également une uniformisation des types de rendez-vous, et donc un consensus entre les médecins. Pour le moment, une plateforme comme *Doctolib* a réussi à imposer un tel cadre à ses adhérents ; ce n'est pas le cas dans les hôpitaux publics. Sans cette harmonisation en amont des pratiques, il est illusoire de penser que l'harmonisation des SI est possible, sinon à prendre le risque de créer un système dysfonctionnel selon le principe du GIGO (*Garbage In, Garbage Out)*[81].

Si elle est souhaitable et porteuse d'améliorations sensibles de la qualité et de la sécurité des réseaux, l'intégration des SI dans les GHT risque de ne pas être effective à court terme.

3.3 Conclusion

Le Directeur d'hôpital doit jouer le rôle de stratège de la cybersécurité. A ce titre, il lui revient de prendre le recul suffisant pour appréhender les grands principes du fonctionnement d'un système d'information, et, dès lors, prendre des décisions concernant l'inclusion de l'informatique dans le système d'information. De façon pragmatique, c'est la question de l'équipement en objets connectés qui va se poser aux managers hospitaliers dans les années à venir, et c'est là que le Directeur va devoir décider de l'opportunité et des modalités de ce virage. De la même manière, c'est à lui qu'il revient d'organiser les équipes pour que les nouvelles fonctions créées par les institutions jouent pleinement leur rôle. C'est donc au Directeur, en définitive, qu'il incombe de créer les conditions pour que la cybersécurité ne soit plus seulement un aspect du travail d'une DSI, mais un projet transversal et une valeur ajoutée pour les patients.

[81] Des entrées incohérentes dans un système mènent à des résultats incohérents à la sortie.

CONCLUSION

La cybersécurité ne se cantonne pas au périmètre du DSI. Si l'on admet qu'elle sera un enjeu majeur des prochaines années, il est indispensable que toutes les directions se saisissent du sujet, *a minima* pour en prendre la mesure, idéalement pour contribuer au développement d'une « conscience » informatique qui, pour le moment, fait défaut globalement dans les établissements de santé.

La menace, on l'a vu, existe déjà et elle est appelée à s'amplifier car le mouvement général est celui d'une connexion de plus en plus complète des systèmes d'information au réseau. La multiplication des objets connectés va encore accroître le nombre et l'intérêt des données de santé ; dans le même temps, le nombre d'objets connectés va augmenter le nombre de possibilités de pénétrer les systèmes d'information pour accéder à ces données. L'absence persistante de *built-in security* dans la conception, le choix et l'utilisation des outils rend inévitable l'explosion du nombre de failles potentiellement exploitables. Parallèlement, la maturité des organisations de santé en matière de cybersécurité et le niveau d'appropriation des enjeux par les agents et les *managers* peuvent laisser craindre une augmentation nette des incidents, à la fois accidentels et volontaires.

La première façon de pallier ces manques et de se protéger de la menace cyber est de suivre la réglementation complexe qui a été mise en place depuis une décennie. Le respect de cette réglementation, notamment en ce qui concerne la cartographie des risques et les PCA, relève principalement de la DSI et du RSSI. Les autres directeurs ont, en revanche, un rôle à jouer en ce qui concerne la formation et la préparation aux situations de crise. Le soutien de la Direction générale est indispensable pour que les campagnes d'information et de formation prennent tout leur sens et portent leurs fruits. En l'absence de ce soutien institutionnel, la sécurité des systèmes d'information risque d'être réduite à une liste de mesures contraignantes et rébarbatives. Un réel effort de pédagogie doit être fait pour que la cybersécurité prenne un sens aussi concret dans les pratiques que, par exemple, l'identito-vigilance.

Le Directeur d'hôpital, enfin, a tout intérêt à organiser ses services de façon à prendre en compte le critère de la cybersécurité dans tous les projets menés. Ainsi, la séparation hiérarchique entre DSI et RSSI permet au RSSI de jouer un rôle de contrôle interne précieux. Une réflexion sur l'opportunité d'étendre la connectivité des systèmes d'information doit être menée sur un pan stratégique, en ayant conscience du risque lui-même, mais aussi de la position de dépendance technologique que va impliquer l'adoption des technologies liées à la 5G. A cet égard, l'inclusion de clauses précises dans les processus d'achat est indispensable L'ensemble de ces mesures contribuera à

repenser le budget de la cybersécurité en intégrant la diminution des risques à un financement appelé, sinon, à être inflationniste. L'exercice consiste donc, pour le Directeur d'hôpital, à considérer les outils informatiques et leur connexion au réseau pour ce qu'ils sont : des outils dont les bénéfices peuvent être immenses à condition qu'on les utilise correctement et qu'on soit, à un moment, en mesure de les considérer avec quelque hauteur – hauteur indispensable pour voir venir les innovations et en évaluer les risques pour l'hôpital et les bénéfices pour le patient.

BIBLIOGRAPHIE

Ouvrages, guides et articles :

ANAP, *Atteindre les prérequis HOP'EN, Boîte à outils*, juin 2019

ANSSI, *Cartographie du système d'information, Guide d'élaboration en cinq étapes,* novembre 2018

APSSIS, *Ouvrage collectif SSI Santé*, janvier 2019

ASSEMBLEE NATIONALE*, Compte rendu de la Commission des affaires européennes*, Audition de Mme Marie-Laure Denis, Présidente de la commission nationale de l'informatique et des libertés (CNIL), 27 juin 2019

BADA Maria, SASSE Angela M. et NURSE Jason R.C., « Cyber Security Awareness Campaigns: Why do they fail to change behavior? », *International Conference on Cyber Security for Sustainable Society*, 2015

BOUQUOT Brigitte (AMRAE), POUPARD Guillaume (ANSSI), *Maîtrise du risque numérique : l'atout confiance*, sans date de publication

CARTAU Cédric, *La sécurité du système d'information des établissements de santé*, Presses de l'EHESP, 2ème édition, 2018

COMMISSION EUROPEENNE, *Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux*, 10 juin 2020

DEMAISON Stéphane et alii, « Panne de téléphonie : gestion de crise, retour d'expérience à l'hôpital Bégin », *Techniques hospitalières*, mars-avril 2019

Direction Générale de l'Offre de Soins, *Memento à l'usage du Directeur d'établissement de santé - Cybersécurité : connaître vos risques pour mieux y faire face,* 2017

EENA, *Cybersecurity : Guidelines and Best Practices for Emergency Services*.

HENNION Sylvie, « le partage du secret professionnel à l'heure du numérique », RDSS, janvier février 2020

Hôpital, Police, Justice (Dossier), *Gestions hospitalières*, Numéro 540 - novembre 2014

HUTCHINS, CLOPPERT et AMIN, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, LockeedMartin, 2010

KAPLAN, James M, et. al. *Beyond Cybersecurity : Protecting Your Digital Business*. NY, John Wiley and Sons, 2015

Ministère des solidarités et de la santé, HFDS, ANS. *Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur de la santé*, Rapport public 2019

NURSE Jason, CREESE Sadie, GOLDSMITH Michael, LAMBERTS Koen, "*Guidelines for Usable Cybersecurity : Past and Present", Conference paper 2011*

ORANGE CYBERDEFENSE*, Potential risks for the pharmaceutical sector*, ORANGE CYBERDEFENSE Epidemiology Lab, OSINT Unit, 29 avril 2020

ORANGE CYBERDEFENSE, *The Threat of Cyberattacks on healthcare establishments during the Covid-19 pandemic*, ORANGE CYBERDEFENSE Epidemiology Lab, OSINT Unit,

PUJOLLE Guy, *Les réseaux, 9ème édition, L'ère des réseaux cloud et de la 5G, 2018-2020*, Eyrolles, 2018, Paris.

RADWARE, *Hacker's Almanac : a field guide*, 2019

SGDSN, *Revue stratégique de cyberdéfense*, 12 février 2018,

SORAYA Sidani, *Intégration et déviance au sein du système international*, Presses de Sciences Po, « Relations internationales », Paris, 2014

VERIZON, *2019 Data Breach Investigation Report*, 2020

WILDE Gerald JS, « Risk Homeostasis Theory: An Overview » *Injury Prevention,* July 1998

ZORN-MACREZ C, *Chroniques martiennes des données de santé numérisées : brèves observations sur une réglementation surréaliste,* RDS n°36, 2010, 331

Sites Internet :
Presse générale et spécialisée :

InfoSanity et *Zataz* : Blogs spécialisés en cybersécurité
https://blog.infosanity.co.uk/
https://www.zataz.com/

TIC Santé : magazine spécialisé en technologies de d'information et de la communication dans le domaine de la santé

http://www.ticsante.com/

APM News, *HospiMedia* et *HealthCare Info Security* : sites de presse spécialisée santé

https://www.apmnews.com/

https://abonnes.hospimedia.fr/

https://www.healthcareinfosecurity.com/

Reuters : agences / titres de presse généraliste

https://www.reuters.com/

Titres de presse généraliste : *Financial Times, Mediapart*

https://www.ft.com/

https://www.mediapart.fr/

Sites institutionnels

https://eena.org/

https://www.ssi.gouv.fr/

https://services.renater.fr/

https://www.coe.int/

https://www.interpol.int/

Sites commerciaux

https://www.lockheedmartin.com/

https://www.iso.org/

https://caih-sante.org/

https://www.microsoft.com/security/blog/

LISTE DES ANNEXES

Annexe 1 : liste des personnes rencontrées :

Mme Béatrice Bérard, OSSI des HCL

M. Marc Bérard, DPO des HCL

M. Cédric Cartau, RSSI et DPO du CHU de Nantes

M. François Daviot, Commissaire de Police

M. Sylvain François, DSI au CHU de Rouen

M. Ludovic Jamart, *Orange Cyber Defense*

M. Frédéric Loudenot, HFDS des Ministères sociaux

M. Bruno Perrier, Capitaine de Sapeurs-Pompiers, SDMIS du Rhône

M. Nicolas Ritouet, Informaticien

M. Erwan Trividic, Directeur des relations extérieures, SHAM

Annexe 2 : Glossaire des termes techniques

AD, *Active Directory :* répertoire complet des profils utilisateurs et des accréditations au sein d'une structure.

Antivirus : logiciel chargé de comparer les flux entrant dans l'ordinateur à la base de données des virus connus : une qlerte est lancée lorsqu'un code est reconnu comme malveillant.

APT, *Advanced Persistent Threat* (menace persistante avancée) : type d'opération de piratage informatique caractérisé par sa complexité et sa furtivité. Par extension, l'acronyme est repris, augmenté d'un nombre, comme nom de groupe de hackers. Ceux-ci se font également connaître sous les initiales TA suivies d'un nombre, pour *Threat Actor* (TA505).

Big game hunting (Chasse au gros gibier) : type de piratage ciblant uniquement les victimes d'envergure (à la différence des attaques massives et indifférenciées).

BotNet : « réseau robot » : un *BotNet* est un réseau virtuel malveillant mis en place grâce à une intrusion furtive par laquelle un ordinateur prend le contrôle de nombreuses autres machines, qualifiées de « zombies », afin de mettre à profit leur puissance de calcul pour lancer une attaque coordonnée (par exemple, une attaque en DDoS)

Couche logique / couche sémantique : Le réseau Internet est constitué, sommairement, de trois niveaux ou couches, qui correspondent à un mode de transmission des données. Le niveau bas est la couche physique : il s'agit des infrastructures filaires, des câbles de cuivre. Le deuxième niveau est la couche logique : cette couche, invisible pour l'utilisateur, est celle de la transmission numérique des données entre serveurs et entre réseaux. La couche sémantique est le niveau haut, auquel l'utilisateur a accès. C'est celui du contenu alphanumérique dans une langue donnée et du *multimedia*.

Clickbait (piège à clics) : on désigne par ce terme un contenu web – mot, image… – conçu pour attirer un utilisateur et le pousser à cliquer dessus : il peut s'agir de mots ou de contenus particulièrement provocateurs, ou de photographies intrigantes. Ces *clickbaits* permettent d'attirer l'utilisateur sur des pages non sécurisées où l'utilisateur risque de révéler à son insu des informations réutilisées par la suite.

Cryptolocker ou **cryptovirus** *:* code malveillant capable d'encoder les données d'une machine afin de les rendre indisponibles. La victime d'une attaque de ce type doit payer une rançon en cryptomonnaie pour récupérer ses données.

DDoS*; Distributed Denial of Service* (Déni de service distribué)

Défacement : manœuvre malveillante consistant à prendre le contrôle d'une page web, souvent la page d'accueil d'un site, pour en modifier ou en caviarder le contenu avec des messages revendicatifs.

EDR, *Endpoint Detection and Response :* système de sécurité qui s'ajoute au Firewall et à l'antivirus, consistant à analyser les flux entrant et sortant afin de repérer des anomalies dans les mouvements pouvant suggérer l'action d'un logiciel malveillant.

Firewall : système de défense reposant sur l'ouverture et la fermeture de ports permettant de limiter les flux de données entrant sur une machine.

IAM, *Identity Access Management* : logiciel de gestion des accréditations, dont dépend l'AD. L'IAM est considéré comme un méta-annuaire.

Ingénierie sociale : technique de manipulation reposant sur l'établissement d'une relation de confiance avec un agent dont le pirate veut soutirer des informations. Dans le pire des cas, la technique permet de se faire remettre les codes et identifiants sous couvert de maintenance informatique. Généralement, elle permet de collecter des informations réutilisées pour renforcer la crédibilité du pirate.

IoT, *Internet of Things* : nom générique donné à la famille des objets connectés, catégories de matériel déjà en usage susceptibles d'être raccordés à Internet grâce à la transmission *WiFi* de 5ème génération, la 5G. Les montres connectées appartiennent à cette catégorie. A terme, les pousse-seringue ou les robots chirurgicaux pourraient en faire partie.

Kit « exploit » : un *exploit* est une faille demeurée secrète d'un programme. L'utilisation de l'*exploit* permet de pénétrer le programme sans difficulté mais cela attire immédiatement l'attention sur son existence. Un kit « exploit » constitue une méthode de pénétration d'un programme particulier dont des failles existantes n'ont pas été réparées.On peut se procurer le kit sur le *Darknet*.

OS, *Operating System* : code selon lequel une machine fonctionne. Les OS peuvent dépendre du fabricant ou non : les appareils Apple fonctionnent selon l'OS d'Apple, MAC OS. Les autres machines utilisent l'environnement Microsoft, Windows. D'autres systèmes d'exploitation, comme Unix, existent concurremment. Ces systèmes d'exploitation équipent par défaut les machines, qui peuvent ou non communiquer entre elles avec plus ou moins de fluidité.

Phishing (hameçonnage) et *spear phishing* : le *phishing* est une technique d'attaque consistant à appâter par mail un utilisateur en le poussant à donner des informations personnelles permettant de s'introduire dans un système. C'est une des techniques de l'ingénierie sociale. Le *spear phishing* est une déclinaison personnalisée du *phishing* qui cible une personne ou un groupe en particulier.

ransomware *:* voir *cryptolocker*

RDP, *Remote Desktop Protocol* : Protocole permettant de prendre le contrôle à distance d'une machine. Utilisé par l'assistance informatique pour aider les utilisateurs, ce système peut aussi être détourné pour un usage malveillant soit par intrusion dans la couche

logique, soit par ingénierie sociale, en se faisant pour un technicien de l'assistance informatique.

SCADA, *Supervisory Control And Data Acquisition :* logiciel de maintenance industrielle avancée permettant la surveillance à distance des installations et l'action, automatisée ou non, sur les outils physiques.

SDN , *Software-Defined Networking* : le SDN se fonde sur le *cloud computing* : il consiste à concevoir les réseau non pas à partir d'une couche physique, mais à l'intérieur d'un *cloud* afin de rendre le réseau plus souple et plus performant. La plupart des composantes physiques du réseau deviennent dès lors des composantes virtuelles (routeur, répéteur…). Contrairement à la structure décentralisée des réseaux actuels, le SDN se caractérise par sa centralisation.

Security by design : mode de fabrication consistant à intégrer la sécurité à l'architecture du logiciel, au lieu de construire un logiciel ouvert auquel on ajoute, ensuite, des sécurités.

TCP/IP : *Transmission Control Protocol/Internet Protocol :* mode majoritairement utilisé pour la transmission des données au sein de la couche logique ; langage d'Internet à proprement parler. La communication des données entre utilisateurs repose en particulier sur l'attribution à chacun d'une adresse IP.

Trojan Horse (Cheval de Troie) : logiciel malveillant d'apparence anodine, il inspire confiance mais déclenche un code délétère une fois téléchargé et installé sur une machine.

VPN *Virtual Private Network* : un VPN est un logiciel permettant de créer un tunnel sécurisé entre un utilisateur et un réseau local éloigné. Le VPN est également utilisé pour camoufler une adresse IP derrière une autre adresse IP, afin de brouiller l'identification d'un utilisateur.

UNIX : famille de systèmes d'exploitation à laquelle appartient Linux. MAC OS est un dérivé d'Unix.

Annexe 3 : Résultats du sondage mené auprès des DH et EDH.

1. En tant que directeur, vous sentez-vous concerné par la cybersécurité ?

oui	42
Non	2

2. Vous est-il déjà arrivé de retarder un projet pour des raisons de sécurité informatique insuffisante ?

oui	22
Non	22

3. Vous arrive-t-il de brancher des clefs USB ou disques durs externes ne provenant pas de votre organisation sur vos appareils professionnels ?

oui	34
Non	10

4. Selon vous, le RGPD est-il lié à la cybersécurité ?

oui	33
Non	11

5. Vous arrive-t-il de laisser allumé votre ordinateur en quittant le bureau ?

oui	24
Non	20

6. Vous arrive-t-il de vous interroger sur la conformité au RGPD des projets que vous menez ou auxquels vous participez ?

oui	35
Non	7
Sans objet (les projets n'ont manifestement pas de versant RGPD)	2

7. Si votre écran affiche un message du type "Vous avez été piraté, vos données sont bloquées…", que faites-vous en premier ?

Je coupe l'alimentation électrique / je force l'arrêt de mon ordinateur portable	10
Je ne fais rien, c'est à la DSI d'agir	2
Je passe en mode avion / je débranche le câble d'alimentation d'internet	6
J'appelle la DSI	26

8. Avez-vous déjà entendu parler de l'ANSSI ?

oui	35
non	9

9. Votre établissement fait manifestement l'objet d'une cyberattaque : quelle est la première réaction à avoir ?

Je rends compte sans délai à l'ARS	17

Je rends compte sans délai à l'ANSSI	26
Je rends compte sans délai au HFDS du SGMAS du MSS	1

10. D'après vous, un antivirus protège-t-il de tous les virus ?

oui	2
non	42

11. Faites-vous une différence entre un antivirus et un pare-feu (firewall) ?

oui	29
Non	15

12. D'après vous, un VPN protège-t-il contre les virus ?

oui	3
non	41

13. Savez-vous qui est l'AQSSI de votre établissement ?

oui	12
Non	32

14. Lors d'un appel d'offre concernant un équipement connecté au SI, avez-vous déjà demandé des garanties de sécurité informatique de la part du futur prestataire ?

oui	31
non	13

15. Savez-vous qui sont le DPO et le RSSI de votre établissement ou de votre structure ?

Oui, les deux.	16
Oui, une même personne a les deux fonctions.	5
Un des deux.	12
Non	11

16. Sélectionnez la proposition qui correspond le mieux à votre pratique :

Je fais plus attention au risque cyber avec mon équipement personnel (parce que c'est le mien, et que la DSI s'occupe de l'équipement professionnel)	4
Je fais plus attention au risque cyber avec mon équipement professionnel	5
Je suis aussi attentif et prudent avec les équipements professionnels qu'avec les équipements personnels.	29
Je suis aussi ignorant des enjeux avec les uns qu'avec les autres.	4
Autre	2

17. D'après vous, le déploiement futur de la 5G en santé est :

Une formidable opportunité	10
Un péril imminent	6
Sans opinion	28

18. En quelques mots, quelle serait selon vous la principale conséquence d'une attaque informatique réussie ?

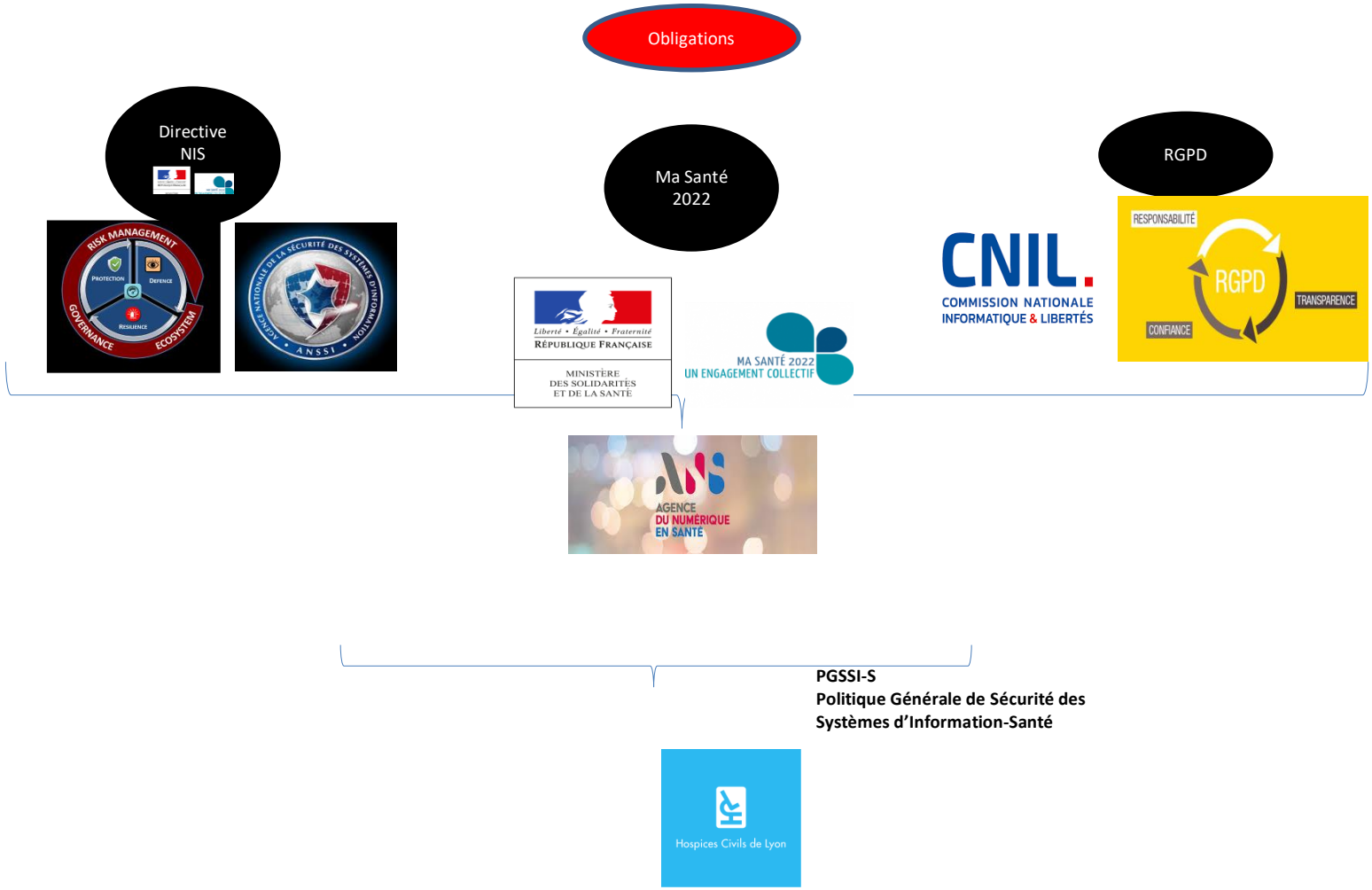
19. Quelle fonction exercez-vous ?

DH en exercice	6
EDH	36
DSI	1
Autre	1

20. Dans quel type de structure exercez-vous ?

CHU	13
CH	31
Autre structure	0

Annexe 4 : le cadre juridique de la protection des données (Source : présentation prévue de l'auteur du mémoire aux instances)



Politique de Sécurité des Systèmes d'Information

Annexe 5 : scénario commenté d'un exercice de crise cyber.

INJECTS

temps	Emetteur animation	Récepteur	Mode de transmission	Objectif	*Injects* d'évènements	Réactions attendues	Observations
h-2h	Avant le début du jeu			Déterminer la réalité d'une attaque cyber	Les écrans affichent tous : « Vos données ne sont plus accessibles. Elles ne sont pas perdues. Pour les récupérer, il vous suffit de … » Le réseau est coupé		L'exercice commence lorsque la CCH est réunie et complète. NB : théoriquement, le réseau téléphonique peut être neutralisé par l'attaque. Le choix est fait de laisser la téléphonie active afin de ne pas compliquer l'exercice. En cas de coupure des DECT, les téléphones restent utilisables avec des numéros à 10 chiffres mais il n'existe pas d'annuaire papier largement diffusé permettant de les récupérer.
H				Constituer une cellule de crise adaptée à l'événement	Cellule de crise hospitalière HCL ouverte, participants arrivés.	Organisation de la cellule de crise	
		DSI	téléphone	Déclencher la déconnexion totale du réseau	DSI expose la situation et propose la coupure générale	Coupure du réseau totale / bascule sur les procédures dégradées	L'interconnexion des SI impose que la coupure du réseau dans sa totalité soit décidée, même si seule une portion du réseau semble touchée. En l'absence d'information, il n'est pas envisageable de tenter de maintenir en marche les secteurs qui semblent sains.
H+5'	Services	Directeurs GH ?	téléphone	Tester la mise en place des procédures dégradées	Les ordinateurs de sauvegarde sont inutilisables Les appels au 654 affluent, saturation	Dépêcher des agents sur place pour donner les instructions ; Organiser le détournement des urgences ; Organiser l'annulation du programme opératoire	Du fait du faible niveau de maturité des organisations, la mise en place de procédures dégradées sera forcément inopérante : les ordinateurs de sauvegarde étant connectés au réseau, ils sont également rendus indisponibles. Il est important d'avoir sur place des relais qui expliquent ce qu'il se passe (Retex Rouen).
H+10'	DSI	DSI	téléphone	Organiser la communication	DSI prévient : il s'agirait d'un virus par un mail malveillant ; provenance : un établissement du GHT qui délègue sa gestion RH aux HCL (adhérent Arhpege) ; ouverture du mail à la DPAS.	Contact avec le directeur de l'établissement partie du GHT et les autres ;	Suivi des remédiations internes et externes. L'isolement avec l'établissement externe sera maintenu après réouverture.

H+20'	Anssi	rssi	téléphone	Evaluer le degré de confidentialité de l'information.	Contact RSSI / ANSSI = données de l'établissement en partie accessibles sur Internet (copies d'écran du service d'imagerie) : menace des pirates ; L'ANSSI demande qu'aucune information concernant le détail de l'attaque ne soit divulguée.	Organiser la communication de crise Alerter le DPO	Dans le cas d'une demande de rançon, la divulgation de données de santé partielles permet de crédibiliser la menace.
H+30'			téléphone	Faire face à la réaction du public	Un médecin annonce qu'un de ses confrères a entendu parler d'une fuite de données personnelles sur Internet / liste de patients circule	Quelle réactivité aux fausses nouvelles divulguées ? Quelle réaction ?	Retex Rouen : les fausses nouvelles ont beaucoup circulé autour de l'incident. Des personnels de l'établissement ont pu choisir de suivre des conseils venus des réseaux sociaux plutôt que les instructions de la direction, concernant par exemple la déconnexion des PC.
H+40'			téléphone		Premières brèves dans la presse et sur les réseaux sociaux ; fausses informations divulguées		
H+50'	Service réa	Directeur GH ?	téléphone		Les respirateurs de réa dysfonctionnent + absence de remontée d'alerte (bip pas entendu) : un mort.	Ne rien dire	La fermeture du réseau désactive le fonctionnement des systèmes d'alerte : les respirateurs fonctionnent encore, mais pas les répétiteurs de sonnettes permettant d'alerter les salles de soin.
H+55'	Collègue DG APHM	DG	Téléphone personnel		Demande d'information sur les modalités de l'attaque	Ne rien dire	
H+60'	PCS	DPSG	téléphone	Faire face à la réaction du public	Nombreux journalistes tentent d'entrer dans les services	Bloquer les accès ; renforcer le contrôle d'accès aux bâtiments en dépêchant des personnels ; filtrage à l'entrée des sites.	Retex Rouen : gros afflux de journalistes désireux de prendre contact avec des agents ou d'entrer dans les services de soin. La déconnexion du réseau entraîne l'ouverture par défaut de tous les accès. Plus de possibilité de fermeture générale à distance par MicroSesame.
H+70'	GIE Hopsis	SG ?	téléphone	Faire face à la réaction des clients et des collègues informés.	Les clients Easily veulent avoir des informations	Ne rien dire.	La prise en main par l'ANSSI déclenche un black-out total de l'information sur les causes de l'incident. Des collègues susceptibles d'être concernés demandent à être informés mais la consigne du secret de l'enquête doit être maintenue.
H+80'	DSI	DSI	téléphone		La fuite de données était un *hoax* : les listes ne correspondent à rien.	Ne rien communiquer	
H+90'					FINEX		

Annexe 6 : Santé & Biomédical, document *TrendMicro*

LETELLIER	Jean-Roch	<Date du jury>

Filière Directeurs d'hôpital

Promotion 2020

Le rôle du Directeur d'hôpital en matière de cybersécurité

PARTENARIAT UNIVERSITAIRE : <Université VILLE>

***Résumé* :**

Les établissements de santé sont de plus en plus souvent victimes d'attaques informatiques. Quelle que soit la motivation de ces attaques, leur objectif est toujours le même : mettre la main sur les quantités sans cesse croissantes de données de santé, soit pour les voler, soit pour les pervertir, soit pour les rendre inaccessibles. Dans tous les cas, les établissements de santé courent et font courir à leurs patients des risques réels s'ils ne prennent pas la mesure du risque cyber.

Malgré cet état de fait et les expériences de certains établissements qui ont pu constater l'impact des vulnérabilités informatiques sur leur fonctionnement, les personnels hospitaliers n'ont qu'une maîtrise théorique des enjeux, et ont tendance, à tous les niveaux, à considérer que la cybersécurité est du domaine exclusif de la DSI et des informaticiens.

Ce mémoire part du principe que cette attitude n'est pas adaptée aux défis du *big data* en santé, et que la cybersécurité a vocation à devenir un véritable enjeu de gouvernance, qui concerne autant la sécurité des patients que celle des établissements. A cet égard, le Directeur d'hôpital à l'heure de la *e-santé* n'a d'autre choix que de promouvoir autour de la cybersécurité un ensemble de projets grâce auxquels pourra s'accroître la maturité des organisations.

Ce mémoire tend à montrer, à partir d'observations et d'enquêtes menées aux HCL et dans d'autres établissements, que les aspects techniques de la cybersécurité sont impuissants à protéger le Système d'information hospitalier sans l'appui d'un *top management* : celui-ci doit être à même d'organiser les structures hospitalières de façon à affronter les évolutions inhérentes à la technologie des réseaux avec souplesse et efficacité.

***Mots clés* :**

Cybersécurité, système d'information hospitalier, gestion du risque, cellule de crise, formation