Outiller l'ingénieur biomédical dans la prévention des cyberattaques

Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin

Université de Technologie de Compiègne
Master 2 - Ingénierie de la Santé
Technologies Biomédicales et Territoires de Santé
Année Universitaire 2023/2024 - Janvier 2024

OUTILLER L'INGÉNIEUR BIOMÉDICAL DANS LA PRÉVENTION DES CYBERATTAQUES

Auteurs :
Benoît BARBIER
Marie BOSSARD
Marion DURAND
Thomas ROBIN

Tutrice :
Julie FOLLET

Mémoire d'Intelligence Méthodologique

Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

DOI : https://doi.org/10.34746/ids213

DOI : https://doi.org/10.34746/ids213

Tables des matières :

DOI : https://doi.org/10.34746/ids213

Remerciements

La concrétisation de ce projet a été possible grâce à la collaboration et à l'engagement d'un groupe de contributeurs qui ont généreusement apporté leur soutien. Nous exprimons notre profonde gratitude envers tous ceux qui ont participé à la réalisation de ce projet et notamment les différents professionnels qui ont accepté de faire des entretiens.

Nous tenons également à remercier l'ensemble de l'équipe pédagogique du Master Ingénierie de la Santé de l'Université de Technologie de Compiègne.

Nous remercions notre tutrice de projet Madame Julie Follet, pour l'ensemble de ses retours sur nos productions, ses conseils et son accompagnement. Nous remercions également les responsables du Master, Madame Isabelle Claude, et Monsieur Jean-Matthieu Prot, pour leur attention particulière ainsi que pour leurs recommandations.

Enfin, nous exprimons notre sincère gratitude à l'ensemble des ingénieurs et techniciens biomédicaux qui ont pris de leur temps pour nous aider à élaborer ce projet ainsi que pour leurs retours constructifs sur nos productions.

Table des illustrations :

DOI : https://doi.org/10.34746/ids213

Résumé

La numérisation croissante des systèmes d’information dans les services de soins des établissements de santé, a ouvert de nouvelles voies pour l'amélioration des soins. Cependant, cette avancée technologique s'accompagne d'un défi majeur à savoir la cybersécurité au sein de ces derniers. La protection des données médicales sensibles, la préservation de l'intégrité des systèmes informatiques, et la garantie du bon fonctionnement des équipements biomédicaux sont des impératifs cruciaux. Face à l’émergence des risques cyber, il est nécessaire d'outiller les ingénieurs biomédicaux dans la prévention des cyberattaques.

En s'appuyant sur les enseignements de la publication “Sécurité Numérique des équipements biomédicaux" de l'Association Française des Ingénieurs Biomédicaux (**AFIB**), quatre outils ont été élaborés pour favoriser l’intégration de la sécurité numérique dans les procédures d'achat, définir les modalités de collaboration au sein des établissements de santé, assurer la sécurité autour des équipements biomédicaux et évaluer la criticité de ces équipements.

Ces outils ont fait l’objet de tests auprès d’ingénieurs biomédicaux pour vérifier leur adéquation aux besoins de la communauté biomédicale et dégager des perspectives d’évolution.

Abstract

The increasing digitization of information systems in healthcare institutions' care services has opened new avenues for improving patient care. However, this technological advancement comes with a major challenge, namely cybersecurity within these institutions. Safeguarding sensitive medical data, preserving the integrity of computer systems, and ensuring the proper functioning of biomedical equipment are crucial imperatives. Due to emerging cyber risks, it is necessary to equip biomedical engineers with tools for preventing cyber-attacks.

Drawing on the insights from the publication "Digital Security of Biomedical Equipment" by the French Association of Biomedical Engineers (**AFIB**), four tools have been developed to promote the integration of digital security into purchasing procedures, define collaboration modalities within healthcare institutions, ensure security around biomedical equipment, and assess the criticality of these devices.

These tools have undergone testing with biomedical engineers to verify their suitability for the biomedical community's needs and to identify potential areas for improvement.

DOI : https://doi.org/10.34746/ids213

Liste des sigles

AFIB : Association Française des Ingénieurs Biomédicaux

ANSSI : Agence Nationale de la Sécurité des Systèmes d'information

ARS : Agence Régionale de Santé

CERT : *Computer Emergency Response Team* [1]

CESIN : Club des Experts en Sécurité de l'Information et du Numérique [2]

DDoS : *Distributed Denial of Service* [3]

DM : Dispositif Médical

DPO : Délégué à la Protection des Données

DSI : Direction des Systèmes d'Information

ENISA : *The European Union Agency for Cybersecurity* [4]

GHT : Groupements hospitaliers de territoires

GMAO : Gestion de la Maintenance Assistée par Ordinateur

MACE : Méthode d'Analyse de la Criticité des dispositifs médicaux en Exploitation

OS : *Operating System* (Système d'exploitation)

RGPD : Règlement Général de Protection des Données

RSSI : Responsable de la Sécurité des Systèmes d'Information

SI : Système d'Information

VLAN : *Virtual Local Area Network* (Réseau Local Virtuel)

DOI : https://doi.org/10.34746/ids213

Glossaire

Botnets : Ordinateurs zombies intégrés dans un réseau sans le consentement de leurs propriétaires. En plus de leur utilisation pour paralyser le trafic (dans le cadre d'une attaque par déni de service) et propager du spam, les *botnets* peuvent également être exploités dans des activités criminelles telles que le vol massif de données bancaires et d'identité [5].

CESIN (Club des Experts en Sécurité de l'Information et du Numérique) : Communauté regroupant des professionnels de la cybersécurité issus de diverses entreprises et administrations. Son principal but est de collaborer pour renforcer le niveau de préparation des organisations en matière de cybersécurité [2].

CERT (Computer Emergency Response Team) : Équipe spécialisée dans la gestion des incidents de cybersécurité. Son rôle principal est de surveiller, détecter, analyser et répondre aux incidents de sécurité informatique, notamment les cyberattaques, les violations de données et les incidents liés à la sécurité des réseaux et des systèmes [1].

Cryptojacking : Attaque qui consiste à utiliser les ressources informatiques d'un utilisateur ou d'une organisation pour miner des cryptomonnaies sans leur consentement [3].

Cybercriminels : Ce terme englobe toute personne ou groupe qui commet des crimes en utilisant des technologies informatiques ou le cyberespace. Cela peut inclure un large éventail d'activités, allant du vol d'identité, du ***phishing***, du vol de données, du hacking de systèmes, de la diffusion de logiciels malveillants (comme des virus ou des ransomwares), à d'autres formes de cyberattaques et de fraudes en ligne [6].

Cyberespionnage : Consiste en des activités malveillantes menées par des gouvernements, des organisations ou des individus pour voler des informations sensibles, souvent à des fins d'espionnage ou de vol de propriété intellectuelle [3].

Cybermafias : Groupes organisés, souvent internationaux, qui utilisent des techniques de cybercriminalité pour commettre des activités illégales à grande échelle. Ils opèrent de manière similaire à des organisations criminelles traditionnelles, mais en exploitant les failles du cyberespace pour mener des activités illégales telles que le vol de données, la fraude, le chantage, voire le sabotage à des fins lucratives [3].

Dark Web : ensemble caché de sites Internet accessibles uniquement par un navigateur spécialement conçu à cet effet. Il est utilisé pour préserver l'anonymat et la confidentialité des activités sur Internet, ce qui peut être utile aussi bien pour les applications légales que pour les applications illégales [7].

Data Breach : Une violation de données se produit lorsqu'une personne ou une organisation non autorisée accède à des données sensibles ou confidentielles, exposant ainsi ces informations à un risque de divulgation ou de vol [3].

***DDoS* (*Distributed Denial of Service*)** : Une attaque par déni de service distribuée vise à submerger un système, un serveur ou un réseau avec un trafic excessif, rendant ainsi les services indisponibles pour les utilisateurs légitimes [3].

ENISA* (The European Union Agency for *Cybersecurity) : Agence de l'Union européenne pour la cybersécurité spécialisée dans la promotion de la cybersécurité en Europe. Sa mission principale consiste à renforcer la résilience des infrastructures informatiques et des systèmes d'information au sein de l'Union européenne [4].

Groupe de pirates : Il s'agit d'un ensemble de personnes, souvent partageant des compétences techniques en informatique et en sécurité. Ces groupes peuvent être formés pour des activités éthiques telles que la recherche en sécurité informatique (hackers éthiques), mais peuvent également être des regroupements de personnes cherchant à exploiter des vulnérabilités pour des raisons illégales (hackers malveillants) [3].

Identity Theft : Le vol d'identité implique l'usurpation de l'identité d'une personne, souvent dans le but de commettre des fraudes financières ou d'autres activités criminelles [3].

Information Leakage : La fuite d'informations se produit lorsque des informations confidentielles ou sensibles sont involontairement divulguées, souvent en raison de vulnérabilités de sécurité ou d'erreurs humaines [3].

Insider Threat : Une menace interne se produit lorsque des individus au sein d'une organisation, tels que des employés, abusent de leur accès privilégié pour causer des dommages intentionnels ou involontaires [3].

Malware* (Logiciel malveillant)** : ***Malware est un terme générique qui désigne tout logiciel conçu dans le but de causer des dommages ou de compromettre un système informatique. Les types courants de malware incluent les virus, les vers, les chevaux de Troie et les ransomwares [3].

Organisations de santé : Des entités ou structures qui opèrent dans le domaine de la santé pour fournir des services, des soins, des traitements, et pour gérer les aspects liés à la santé. Ces organisations peuvent prendre diverses formes et tailles, allant des institutions publiques aux établissements privés, des organismes à but non lucratif aux entreprises commerciales. Leur objectif principal est d'améliorer la santé des individus, des populations ou de gérer les systèmes de santé [8].

Phishing : Technique d'attaque qui implique l'envoi de messages ou de sites Web frauduleux pour tromper les utilisateurs et les inciter à divulguer des informations sensibles, telles que des identifiants de connexion ou des informations de carte de crédit [3].

***Physical Manipulation, Damage and Theft and Loss* (Manipulation physique, Dommage, Vol et Perte)** : Cela fait référence aux atteintes à la sécurité qui impliquent des actions physiques sur le matériel ou les dispositifs informatiques, telles que le vol de matériel, la destruction physique ou la perte accidentelle [3].

Ransomware : Type de logiciel malveillant qui chiffre les fichiers d'un utilisateur ou d'une organisation, puis demande une rançon pour la clé de déchiffrement [3].

Script kiddies : des individus peu expérimentés en informatique qui utilisent des outils, des scripts ou des programmes créés par d'autres, sans réellement comprendre leur fonctionnement interne pour compromettre la sécurité des systèmes informatiques de manière opportuniste [3].

Spam : Envoi massif de messages électroniques non sollicités, souvent à des fins de marketing ou de diffusion de contenu indésirable [3].

VLAN (Virtual Local Area Network) : Méthode de segmentation d'un réseau physique en plusieurs réseaux logiques, permettant d'isoler et de regrouper des dispositifs apparentés, indépendamment de leur emplacement physique, pour améliorer la gestion, la sécurité et l'efficacité des réseaux informatiques [9].

Web-based Attacks : Les attaques basées sur le Web sont des tentatives malveillantes de compromettre des systèmes informatiques en exploitant des vulnérabilités spécifiques liées à des applications Web, des serveurs Web ou des navigateurs Web [3].

DOI : https://doi.org/10.34746/ids213

Introduction

À l'ère de la numérisation croissante des systèmes de santé et plus particulièrement dans les établissements de santé, les ingénieurs biomédicaux sont confrontés à un défi majeur : Sécuriser les équipements biomédicaux contre les menaces croissantes de cyberattaques. En effet, les cyberattaques sont classées au 5e rang des risques les plus importants en 2020 et ces dernières ont encore augmenté depuis la pandémie du COVID-19 atteignant 730 incidents déclarés en 2022 contre 327 en 2018 [10]. L'impact de ces attaques va au-delà de la sphère technologique (atteintes du Système Informatique Hospitalier, des Dispositifs Médicaux - **DM**, des données médicales d'un patient…) en affectant directement les missions des services biomédicaux (maintenance préventive et curative des **DM**, utilisation de la Gestion de la Maintenance Assistée par Ordinateur - **GMAO**…). Ce mémoire explore l'impact des cyberattaques sur le métier d'ingénieur biomédical, en mettant en lumière le contexte global de la cybersécurité en France, l'état des lieux des menaces cyber ciblant les établissements de santé, les conséquences financières de ces cyberattaques et la prise en charge complexe des patients.

Face à l'émergence des risques liés à la cybersécurité dans le domaine de la santé, il devient impératif de doter les ingénieurs biomédicaux d'outils efficaces pour prévenir les cyberattaques. En réponse à ces défis, l'**AFIB** a développé des travaux dans la publication "Sécurité Numérique des équipements biomédicaux". Ce mémoire examine le rôle crucial de ces travaux dans l'élaboration de recommandations et d'outils visant à armer l'ingénieur biomédical dans la prévention de cyberattaques. L'accent est mis sur l'intégration de la sécurité numérique dans les procédures d'achat, la définition de la collaboration au sein des établissements de santé, la garantie de la sécurité entourant les équipements biomédicaux, et l'évaluation de la criticité de ces équipements.

Enfin, ce mémoire se penche sur l'évaluation pratique des outils de cybersécurité créés pour les ingénieurs biomédicaux et mis en place en suivant leurs recommandations. En analysant les retours terrain et en réalisant une évaluation approfondie des pratiques du service biomédical, il met en évidence les implications concrètes de ces outils, identifiant leurs avantages tout en soulignant leurs éventuelles limitations. Cet ensemble de travaux vise à guider les ingénieurs biomédicaux vers une intégration efficace de la sécurité numérique, tout en envisageant des améliorations futures pour renforcer la résilience des systèmes de santé face aux cybermenaces.

DOI : https://doi.org/10.34746/ids213

DOI : https://doi.org/10.34746/ids213

I- Impacts des cyberattaques sur le métier d'ingénieur biomédical

1.1) Contexte global de la cybersécurité en France

Selon l'Agence Nationale de la Sécurité des Systèmes d'information (**ANSSI**) qui est l'agence en France chargée de la veille, de l'alerte et de la réaction aux attaques informatiques, une cyberattaque peut être définie comme une "tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (secrets militaires, diplomatiques ou industriels, données personnelles bancaires), de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information (dont les systèmes industriels)" [11]. Les cyberattaques sont perpétrées par différents types d'acteurs (Figure 1) qui visent majoritairement 3 types de cibles. Tout d'abord les ordinateurs et serveurs isolés ou en réseau reliés ou non à internet, ensuite les équipements périphériques, et enfin les appareils communicants comme les tablettes notamment [11].

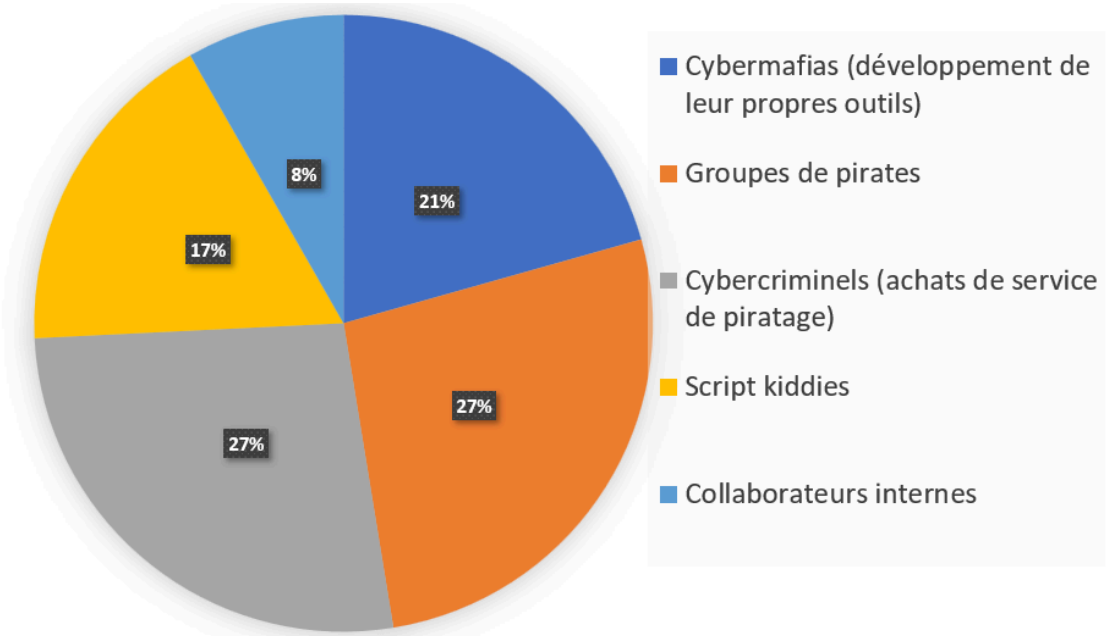


Figure 1 : Répartition des auteurs des cyberattaques (Source : [11]) (Le glossaire peut être consulté pour plus d'informations)

Il existe 4 types de risques cyber que sont le piratage, l'atteinte à l'image, l'espionnage et le sabotage [11]. Le top 15 des menaces les plus observées ces dernières années ainsi que leur tendance croissante ou décroissante est présenté en figure 2.

DOI : https://doi.org/10.34746/ids213

Figure 2 : Top 15 des cybermenaces avec leurs tendances au cours des dernières années (Source : [12])

D'après l'**ANSSI**, les cyberattaques ont connu une augmentation spectaculaire, avec une croissance de 600 % depuis la pandémie du COVID-19, fin 2019, [12] sur tous les secteurs d'activités en France. Cette hausse significative s'explique en grande partie par l'adoption généralisée du télétravail, qui a exposé de nombreuses entreprises à un risque accru d'attaques. En effet, cette pratique a élargi la surface d'attaque à travers l'utilisation de connexions internet non sécurisées et a accru la complexité de la gestion de la sécurité.

En 2021, à travers la plateforme *cybermalveillance.gouv.fr*, un total de 173 000 demandes d'aide de victimes de cyberattaques ont été recueillies, ce qui représente une augmentation de 65 % par rapport à l'année 2020 [13]. Ce nombre de demandes d'assistance a grimpé à près de 280 000 en 2022 [14]. Entre 2021 et 2022 la fréquentation de la plateforme a augmentée de 55% pour atteindre plus de 8.3 millions de vues en 5 ans.

Les données fournies par la plateforme *cybermalveillance.gouv.fr* sont particulièrement intéressantes car sa mission principale est le soutien aux individus, aux entreprises, aux associations, aux collectivités et aux administrations qui sont victimes de cyber malveillance, ainsi que la diffusion d'informations sur les risques numériques et les méthodes pour s'en prémunir. Des chiffres particulièrement informatifs ont été publiés dans le rapport annuel de 2021 de *cybermalveillance.gouv.fr* (Figure 3 et 4). Pour les professionnels, les ***ransomwares* ou rançongiciels** demeurent la principale cause de préoccupation, représentant environ 22 % des demandes d'aide [15].

DOI : https://doi.org/10.34746/ids213

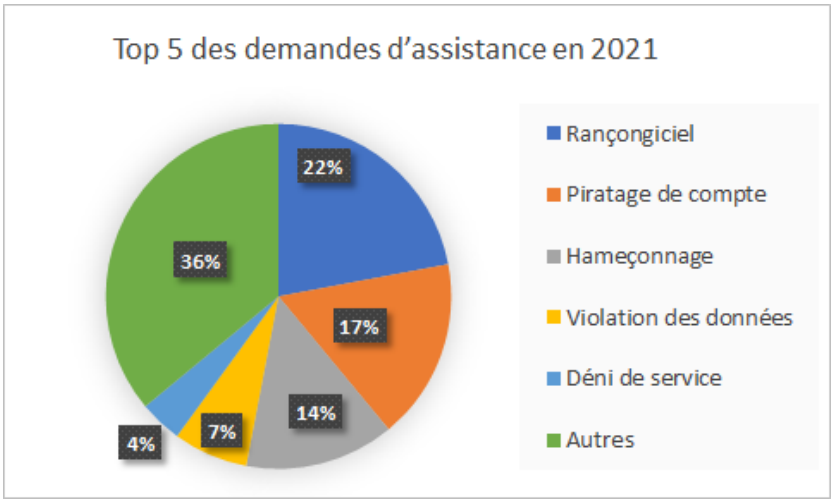


Figure 3 : Top 5 des demandes d'assistance d'après les demandes faites sur la plateforme cybermalveillance.gouv.fr (Source : [16])

Figure 4 : Les grandes menaces de la cybersécurité en 2021 (Source : [16])

En 2022, l'hameçonnage est passé à la première place de chaque catégorie de publics avec une augmentation de 54% des recherches d'informations et d'assistance (Figure 5 et Figure 6) [17].

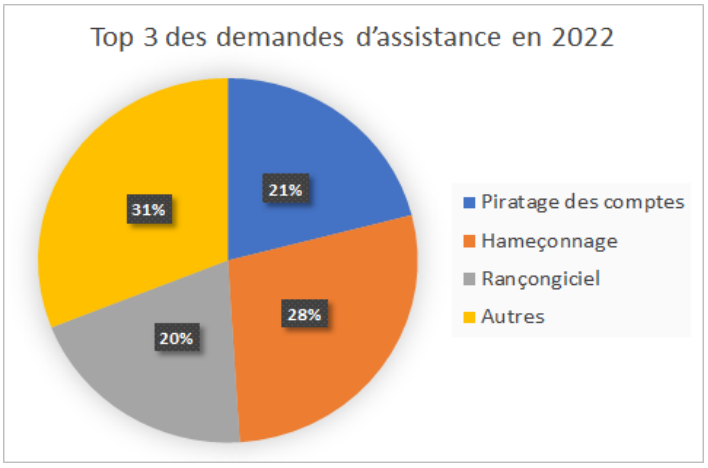


Figure 5 : Tendances des menaces cyber en 2022 d'après les données recueillies sur la plateforme cybermalveillance.gouv.fr (Source : [17])

DOI : https://doi.org/10.34746/ids213

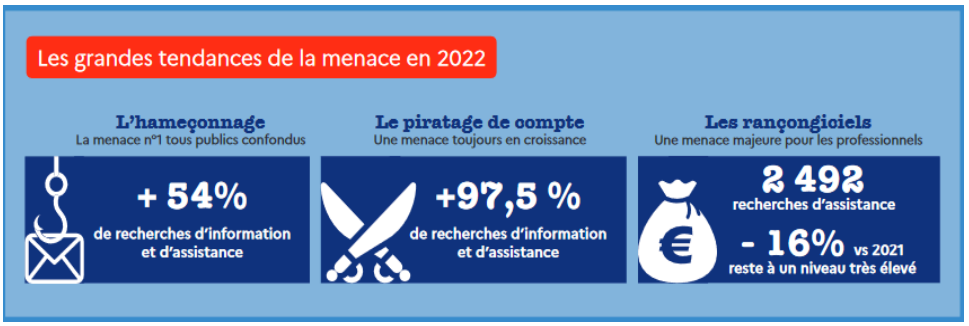


Figure 6 : Les grandes menaces de la cybersécurité en 2022 (Source : [17])

En France, le baromètre du **Club des Experts de la Sécurité de l'information et du Numérique** (**CESIN**) révèle que la moitié des entreprises françaises ont été victimes d'une cyberattaque en 2021. Ces attaques ont un coût non négligeable et croissant au fil des années pour les organismes car selon IBM Security, le coût total moyen d'une violation de données s'élève à environ 3,84 millions d'euros en 2023 en France, comparativement à 3,6 millions d'euros en 2020 [18]. De plus, il est estimé que d'ici 2025, la cybercriminalité coûtera aux entreprises du monde entier environ 10 500 milliards de dollars par an [19].

En 2022, selon l'**ANSSI** les principaux secteurs touchés par les attaques de ***ransomware*** en France étaient les petites et moyennes entreprises (Très Petite Entreprises TPE, Petite ou Moyenne Entreprise PME, Entreprise de Taille Intermédiaire ETI), suivis des collectivités territoriales et des établissements publics de santé (Figure 7) [12]. Les secteurs sont ciblés pour plusieurs raisons tels que la dépendance à l'automatisation et au numérique, le retard en matière de prévention du risque cyber et une insuffisance dans les procédures de reprise d'activité.

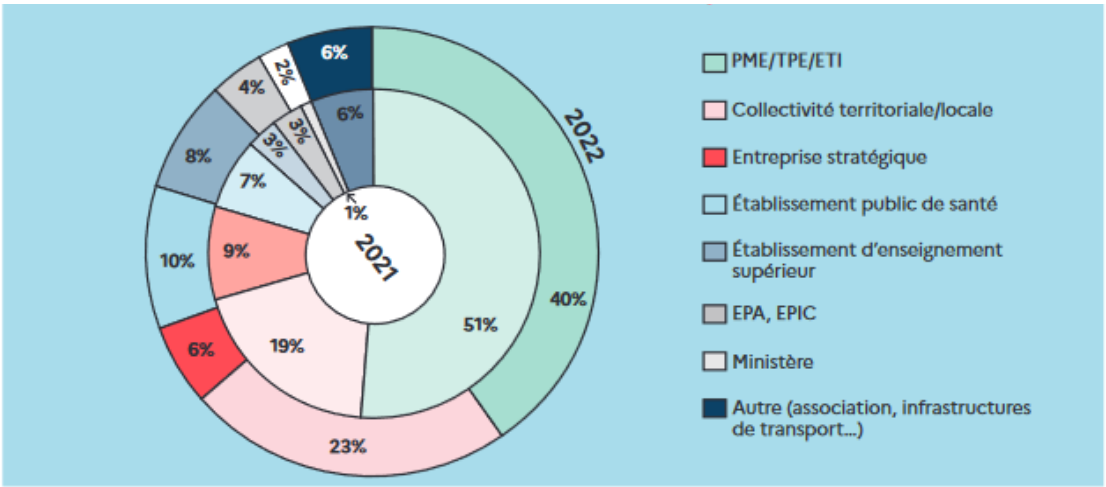


Figure 7 : Répartition des types de victimes de compromissions par ransomwares en 2021 et 2022 (Source : [20])

Ces attaques ont des conséquences importantes notamment sur la diffusion d'informations confidentielles qui alimentent les marchés parallèles. En effet, une étude menée par Sekoia.io (société européenne spécialisée en cybersécurité) au cours du second semestre

2021 révèle que plus de 1000 listes d'accès ont été mises en vente par des hackers utilisant la méthode du rançongiciel. Les prix de ces données varient en fonction de leur nature, par exemple, les données médicales d'une personne se négocient à 200 $, tandis qu'une carte bancaire peut être vendue pour seulement 1 $ car le numéro n'aura plus de valeur lorsque l'usurpation aura été découverte. Selon le secteur d'activité, la taille de l'entreprise et les privilèges d'accès associés, les prix de revente aux enchères peuvent osciller entre 100 et 100 000 dollars par accès. Les cyberattaques ont donc un intérêt financier important, ce qui explique l'augmentation des menaces cyber dans le monde entier [12].

Les acteurs malveillants améliorent constamment leurs techniques à des fins de gains financiers, d'espionnage et de déstabilisation notamment en passant par les équipements périphériques qui offrent un accès plus furtif et persistant aux réseaux des cibles. D'après l'**ANSSI**, les usages numériques non maîtrisés et les faiblesses constatées dans la sécurisation des données continuent d'offrir de nombreuses opportunités d'actions malveillantes. Pour se prémunir des menaces les plus courantes, l'agence préconise notamment l'application d'une politique de mise à jour accrue, une sensibilisation régulière de tous les utilisateurs et le développement de capacités de détection et de traitement d'incidents [13].

1.2) Les cyberattaques au sein des établissements de santé français

1.2.1) Établissements visés

Le nombre d'incidents de sécurité informatique ciblant les établissements de santé a connu une progression constante, avec près de 730 attaques signalées en France en 2021 ce qui équivaut à 2 attaques par jour en moyenne en 2021. En 2022, le ***Computer Emergency Response Team*** (**CERT**) Santé a enregistré 588 déclarations d'incidents de cybersécurité dans les établissements de santé français, mais le même pourcentage de déclarations d'origine malveillante (environ 50%). 27 incidents étaient liés à une attaque par **ransomware** en 2022, contre 59 en 2021 [21].

Les hôpitaux publics se distinguent nettement par une surreprésentation par rapport aux établissements privés (Figure 8). De plus, le **CERT** remarque que la proportion des établissements privés à but lucratif ayant signalé des incidents a été réduite d'un peu plus de la moitié en 2021.

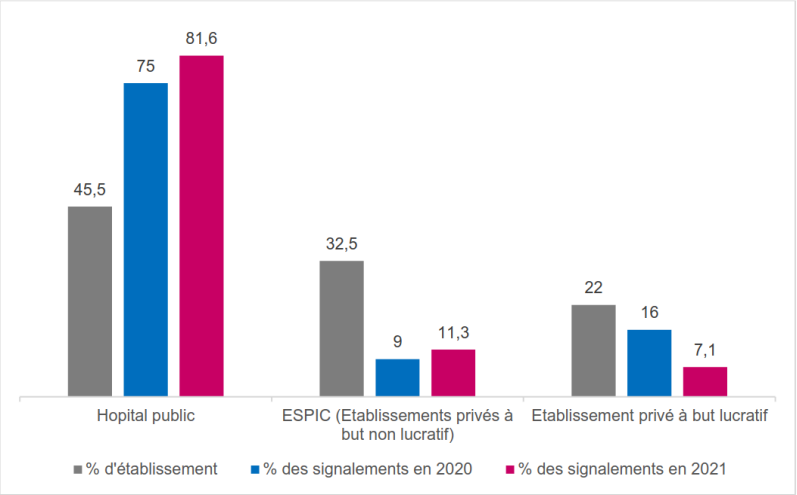


Figure 8 : Part des signalements comparés à la part des établissements selon leur raison social en 2021 (Source : [15])

1.2.2) Attaques ciblant les systèmes d'information

Le risque majeur pour les établissements de santé en France est celui du rançonnage, aussi bien en fréquence qu'en volume puisque ce type d'attaque est passé du 6ème au 1er rang entre 2019 et 2020 [12]. Le rançonnage se caractérise par le chiffrement et l'inaccessibilité des données ce qui désorganise l'activité et la prise en charge des patients, allant même jusqu'à paralyser les services et à la perte de données sensibles. Dans le pire cas, ces cyberattaques peuvent conduire à la mort du patient.
Le rançonnage se pratique de plusieurs façons et notamment par hameçonnage (en anglais ***phishing***), le recours à un identifiant volé lors de précédentes intrusions ou comportements inadaptés, et enfin par l'exploitation de failles de sécurité souvent liées à un système d'exploitation obsolète. Toutes les données collectées peuvent être commercialisées sur les marchés parallèles car les données de santé ont une valeur mercantile très attractive. Ainsi, près de 80 % des attaques étaient motivées par des gains financiers en 2022 [18].

1.2.3) Attaques ciblant les Dispositifs Médicaux exploités

L'essor des solutions de santé numérique permet le partage de données, la surveillance, la prévision des risques, ou encore la gestion des dispositifs et donc le développement de la télémédecine ou des plateformes de suivi des patients. Cependant, les risques associés ne sont pas complètement maîtrisés, ni par les fabricants des **DM**, ni par leurs utilisateurs, ouvrant de nouvelles portes à la cybercriminalité.

En effet, les fabricants peinent encore à posséder une expertise solide en matière de sécurité informatique. Le nombre toujours plus important de **DM** combinés le plus souvent avec des manques en termes de sécurité font des hôpitaux une cible privilégiée pour les cyberattaques. En effet, en 2020, il y avait environ 6 milliards d'objets connectés dans le

monde contre plusieurs centaines de millions d'ordinateurs [23]. L'Agence de l'Union européenne pour la cybersécurité **(ENISA)** en collaboration avec Juniper Research prévoit que d'ici 2026, les **organisations de santé** dans leur ensemble **auront** déployé plus de 7 millions d'appareils médicaux connectés dans le monde, soit le double par rapport à 2021 Au niveau hospitalier, cela équivaut à une moyenne de plus de 3 850 dispositifs par établissement. Ce chiffre représente une croissance totale de 131% par rapport à 2021 [24]. Étant donné que la puissance d'une cyberattaque dépend du nombre de périphériques piratés, il est aisé de comprendre l'intérêt des pirates de réaliser des cyberattaques via ces **DM** connectés mal sécurisés. Ce piratage des **DM** est notamment rendu possible par le fait que les fabricants ont besoin d'avoir un accès à distance pour intervenir sur leur appareil rapidement, risquant de permettre aux hackers de s'infiltrer à leur place [23]. Pendant très longtemps Team Viewer était utilisé mais est maintenant banni de la plupart des établissements du fait de ses nombreux risques en matière de sécurité. La surveillance des **DM** et des réseaux à l'hôpital constitue une tâche complexe pour les services informatiques et biomédicaux. La gestion de ce défi est rendue difficile en raison du volume important de **DM** et de la nécessité de maintenir une connectivité avec des réseaux externes pour des activités telles que la télémaintenance et les mises à jour.

1.2.4) Vulnérabilité des établissements face aux cyberattaques

La croissance de la fréquence et du nombre de cyberattaques touchant les établissements de santé, quelle que soit leur localisation s'explique par leurs vulnérabilités (manque de mise à jour, failles des systèmes d'exploitation et comportements humains à risque... Figure 9). Ainsi, en dépit des idées répandues, les hôpitaux ne sont pas directement visés par les cyber-attaquants qui par opportunisme exploitent une faille de sécurité résiduelle du système informatique. Il y a cependant un réel intérêt, lorsque l'opportunité se présente, pour le caractère sensible et la valeur marchande des données traitées par le système informatique hospitalier (**SIH**) [12].

Figure 9 : Les principales vulnérabilités d'une structure de santé (Source : [25])

L'émergence des risques cyber dans le secteur de la santé s'explique également par le manque de prise de conscience de la part des soignants, submergés de travail et insuffisamment sensibilisés aux différents risques cyber. Par exemple, les soignants ne sont pas forcément au fait que les données médicales ont une valeur marchande très élevée sur le ***Dark Web*** car leur détention permet de demander des rançons, se faire prescrire des médicaments ou usurper une identité [23]. Ces données peuvent également être transmises aux compagnies d'assurances ce qui est très problématique pour le patient.

1.2.5) Conséquences sur les établissements de santé

Les conséquences des cyberattaques sur les établissements de santé sont significatives, puisqu'elles ne se traduisent pas seulement par des pertes financières, mais aussi par une détérioration de la prise en charge des patients et une perte d'intégrité de leurs informations médicales (Figure 10).

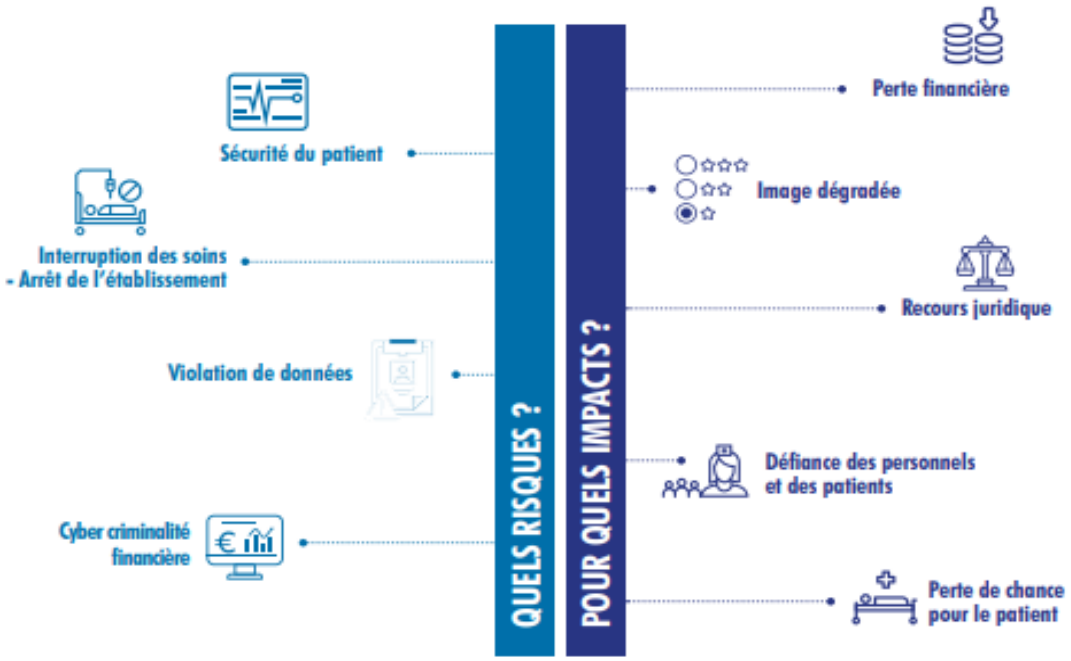


Figure 10 : Les principaux risques et impacts de la cybersécurité en santé (Source : [25])

1.3) Impacts financiers

En 2021, l'hôpital de Dax a été dans l'obligation de déprogrammer des opérations et d'orienter les patients vers d'autres établissements. En plus de la perte de chiffre d'affaires pour l'hôpital, les cyber-attaquants peuvent demander des rançons en échange d'un déblocage du système d'information. En France, il est demandé de ne pas céder au chantage mais dans d'autres pays comme aux Etats-Unis,il n'est pas rare que les établissements acceptent de payer pour débloquer leur système.

La reconstruction de l'environnement numérique est également coûteuse car elle peut prendre plusieurs semaines à plusieurs mois. Les coûts sont donc liés aux ressources humaines mobilisées pendant la gestion de la crise, de nombreux employés doivent faire des heures supplémentaires pour participer à l'effort de crise, et à la commande de prestation informatiques pour accélérer la remédiation. Dans le cas de l'attaque du centre hospitalier d'Albertville Moutiers en décembre 2020, l'impact financier est estimé à 1.5 M€ [11].
En 2019, le CH d'Issoudun dans l'Indre a dû débourser plus de 40 000 euros pour se doter d'un nouveau pare-feu après avoir refusé de payer la rançon associée au virus Antirecuva ANDB [12].
Ce bilan peut s'alourdir dans le cas de sanctions financières prononcées par la Commission nationale de l'informatique et des libertés (**CNIL**) en cas de non-respect du Règlement Général de Protection des Données *(***RGPD**) notamment lors de fuites de données de santé des patients. Selon les données recueillies par le **CERT** en 2021, la répartition des incidents par catégorie de données touchées est la suivante : 56 % ont touché des données de santé à caractère personnel, 34 % des informations à caractère personnel autres que les données patients, 16 % des informations confidentielles ou stratégiques, principalement des identifiants de compte utilisateur, et enfin 12 % des données techniques sensibles [22]. Ces statistiques soulignent que les données personnelles sont les premières touchées par les incidents de sécurité déclarés.

L'étude de 2023, "Menaces et risques cyber pesant sur les établissements de santé en France" conduite par Relyens qui est un groupe mutualiste européen d'Assurance et Management des risques spécialiste des acteurs du soin et des territoires, considère le scénario d'une attaque par rançongiciel d'un établissement de santé de type CHU. Cette dernière suit un mode opératoire classique des **cybercriminels** au cours duquel les attaquants envoient un logiciel malveillant ou un virus à l'établissement, bloquant l'accès à ses données ou à son matériel en les chiffrant [26]. Les criminels exigent ensuite le paiement d'une rançon pour rétablir l'accès. Ce type d'attaque peut entraîner les conséquences suivantes :

- Le chiffrement d'une partie significative du **SIH**, provoquant des perturbations dans les soins, notamment l'indisponibilité du dossier patient informatisé (**DPI**), d'applications métiers et de divers équipements médicaux.
- L'exfiltration de données de santé par les attaquants.

Selon cette étude, l'impact financier d'un tel scénario pour ce type d'établissement est représenté sur la Figure 11.

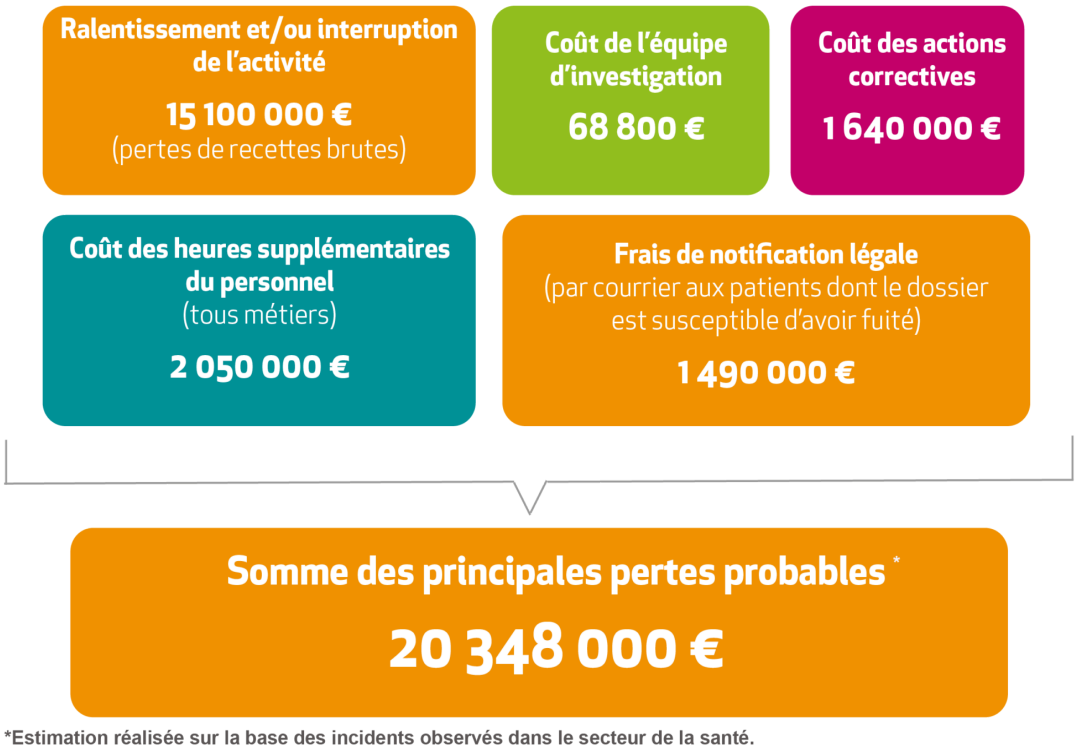


Figure 11 : Estimation de l'impact financier d'une cyberattaque sur un établissement de santé type CHU (Source : [26])

En raison des conséquences graves, tant pour l'établissement que pour la sécurité des patients, il est essentiel que les dirigeants des établissements de santé et leurs **RSSI** aient une vision précise de leur exposition aux risques cyber afin de comprendre les menaces, d'estimer leur niveau et d'évaluer leur capacité de défense afin de mettre en place une politique de cybersécurité adaptée à leur établissement.

1.4) Impacts sur la prise en charge des patients

Un constat préoccupant révèle qu'en 2022, 39% des structures de santé ont dû opérer en mode dégradé pour assurer la prise en charge des patients, mettant en lumière la vulnérabilité du secteur face aux incidents de cybersécurité et la nécessité d'une préparation renforcée. De plus, les conséquences des incidents de cybersécurité en 2022 sont clairement illustrées par le fait que 63% des structures touchées signalent un impact direct sur leurs données, qu'elles soient liées aux patients ou aux opérations internes de la structure [27].

Ainsi, lors d'une cyberattaque, les établissements de santé peuvent se retrouver paralysés. Par exemple, le 10 août 2019, les 120 établissements du groupe Ramsay ont été ciblés par une attaque informatique, affectant les serveurs gérant les infrastructures et les messageries, les rendant inutilisables pendant une période de cinq jours. Cela complique les soins qui sont prodigués au patient puisque la partie numérique est paralysée. Évidemment,

l'organisation peut continuer de fonctionner, même en mode dégradé (papier, téléphone…) mais la prise en charge des patients est tout de même impactée du fait du temps de réorganisation nécessaire des soignants. Le 15 novembre 2019, le **CHU** de Rouen a été gravement touché par une attaque informatique, obligeant l'arrêt de tous les ordinateurs pour limiter sa propagation, provoquant une perturbation significative dans la sécurité et la continuité des soins. Cet arrêt empêche souvent les équipes soignantes de communiquer entre elles comme elles en ont l'habitude ce qui ralentit la continuité des soins et la traçabilité des patients et des actes réalisés.

Un peu plus récemment, en août 2022, le Centre Hospitalier Sud Francilien a été victime d'une attaque par ***ransomware*** qui a entraîné une perturbation majeure de l'accès aux données et aux applications du système d'information, ce qui a rendu très complexe la traçabilité des données du patient et le partage d'informations entre services. Le 23 septembre 2022, environ 11 gigaoctets de données, dont des informations médicales et personnelles concernant les patients et le personnel hospitalier, ont été divulgués sur le site web du groupe de **cybercriminels** à l'origine de l'attaque [28]. Bien que les équipes techniques du Centre Hospitalier, en collaboration avec l'**ANSSI** et divers prestataires, aient réussi à rétablir les services critiques, la reconstruction sécurisée du système d'information et le retour à un fonctionnement normal demandent des efforts à long terme. En effet, le Centre Hospitalier (**CH**) a annoncé un chantier de 12 à 18 mois pour renforcer son infrastructure informatique, mené en collaboration avec l'Agence régionale de santé (**ARS**) [29]. Ainsi la prise en charge des patients n'est toujours pas redevenue optimale et leurs données sont encore présentes à certains endroits du Web. Pour le moment, aucune attaque n'a abouti à la mort avérée d'un patient mais il s'agit d'un scénario tout à fait envisageable.

Ces retours terrains témoignent de l'impact des cyberattaques sur la sécurité des soins et la perte de chances pour les patients. Il s'agit d'une réorganisation complète de l'hôpital qui impacte nécessairement profondément la prise en charge du patient, tout du moins au début de la cyberattaque.

1.5) Mesures de sécurité dans les établissements de santé

La cybercriminalité est devenue une préoccupation prioritaire pour l'hôpital, les patients et la société du fait de la multiplication des attaques et de l'augmentation de leur ampleur. De fait, dans le secteur de la santé émergent de nombreuses réflexions en lien avec la cybersécurité définie alors comme "l'ensemble des mesures techniques ou organisationnelles mises en place pour assurer l'intégrité et la disponibilité d'un **DM** ainsi que la confidentialité des informations contenues ou issues de ce **DM** contre le risque d'attaques dont il pourrait faire l'objet " [30].

La cybersécurité s'appuie sur un triptyque : technique, organisationnel et juridique [31] pour être efficace.

DOI : https://doi.org/10.34746/ids213

1.5.1) Mesures techniques et financières

En 2021, le Président de la République a demandé aux établissements de santé de consacrer 5 à 10% du budget informatique à la cybersécurité. Cette demande suscite plusieurs réflexions. Il faut tout d'abord remettre cela en perspective avec la réalité des budgets des établissements de santé dont le budget est souvent déjà serré pour le fonctionnement global des soins. D'un point de vue critique, on pourrait se demander si l'allocation de 5 à 10% est suffisante, compte tenu de l'évolution constante des menaces cybers. Dans la réalité, les établissements de santé pourraient être confrontés à des défis plus importants et à des coûts plus élevés pour maintenir une cybersécurité efficace. Une évaluation régulière et une adaptation aux nouvelles menaces sont donc essentielles. Cependant cette annonce du Président de la République souligne la reconnaissance de l'importance de la cybersécurité dans le secteur de la santé. Cela est positif puisque les institutions médicales traitent des données sensibles et donc allouer des ressources financières à la protection de ces données est essentiel pour garantir la confidentialité, l'intégrité et la disponibilité des informations médicales. Cependant, il est important de souligner que la cybersécurité ne devrait pas être considérée comme une préoccupation uniquement financière. Elle nécessite une approche complète qui englobe la mise en place de politiques de sécurité, la surveillance constante des réseaux, et la collaboration avec d'autres institutions pour partager des informations sur les menaces. Il est nécessaire que ces fonds soient utilisés de manière judicieuse, en investissant dans des techniques de sécurisation modernes et robustes ainsi que dans des formations adéquates pour le personnel des services informatique, biomédical et de soins. La qualité des investissements est souvent plus cruciale que la quantité.

A ce titre, l'État annonçait en 2021 allouer 25 millions d'euros à l'**ANSSI** pour la réalisation d'audits dans les hôpitaux et 350 millions pour la sécurisation informatique des établissements.
La réalisation d'audits apporte un accompagnement technologique et humain. Effectivement, la réalisation d'audits par l'**ANSSI** dans les hôpitaux vise à évaluer la sécurité des systèmes d'information en place, à identifier les éventuelles vulnérabilités et à formuler des recommandations pour renforcer la posture de sécurité. Ces audits couvrent différents aspects tels que les infrastructures réseau, les applications, les procédures de gestion des accès. Ainsi, ils fournissent une base pour mettre en œuvre des mesures correctives ciblées. Les 350 millions d'euros dédiés à la sécurisation informatique des établissements de santé permettent de financer des initiatives plus larges, telles que l'acquisition de technologies de sécurité, la formation du personnel, la mise en place de procédures de réponse aux incidents, et la création d'une culture de sécurité au sein des établissements.
D'après le Ministre délégué de la Transition Numérique, la démarche a permis de doubler le nombre d'établissements de santé qui bénéficient du parcours de sécurisation des établissements. Mais les financements ayant été octroyés en 2021 il y a pour le moment assez peu de retours d'expérience sur l'efficacité de ces financements. Il serait donc intéressant de recenser ces retours et d'en faire une synthèse pour guider les pouvoirs publics.

Concernant des mesures techniques autres que financières, la Haute Autorité de Santé (HAS) a révisé en fin d'année son guide de certification des établissements de santé vis-à-vis la qualité des soins dispensés en incluant la prise en compte de la gestion des risques numériques dans la prestation des soins. La version la plus récente du manuel de certification élève le niveau d'exigence en intégrant la gestion des risques numériques en tant que critère standard (critère 3.6-02) pour évaluer la qualité des soins dispensés par les établissements de santé à partir du 1er janvier 2024. Ce critère guidera l'appréciation de la qualité des soins prodigués par les établissements de santé, et permettra l'évaluation de critères impératifs comme le 3.6-01 (La gestion des tensions hospitalières et des situations sanitaires exceptionnelles est maîtrisée) et le 3.7-03 (L'établissement analyse, exploite et communique les indicateurs qualité et sécurité des soins).

Le critère 3.6-02 dont le titre est "Les risques de sécurité numérique sont maîtrisés" est donc central. Les éléments d'évaluation de la gouvernance pour obtenir la certification portent notamment sur la présence de plans de continuité d'activité et de reprise d'activité, les actions de sensibilisation régulières pour les professionnels de santé. On retrouve également la désignation de référents sécurité SI formés dans les secteurs à risques et la déclaration immédiate des incidents de sécurité des SI à l'Agence du Numérique en Santé (ANS). Concernant les professionnels, on retrouve la connaissance des procédures en cas d'incident/attaque, la connaissance du contact du référent de la sécurité numérique ou encore la sensibilisation à la suppression de documents de santé avec données personnelles sur les postes de travail.

1.5.2) Mesures organisationnelles

a) Cadre des mesures organisationnelles

La cybersécurité ne se limite pas à l'acquisition du meilleur matériel mais elle repose sur une organisation structurée par le système de management de la sécurité de l'information (norme ISO 27001) [13].

Les mesures organisationnelles se concentrent sur les aspects humains, administratifs et structurels de la cybersécurité, c'est-à-dire à la mise en place de bonnes pratiques et le suivi de la réglementation à l'échelle d'un établissement. Il s'agit de former et de sensibiliser les professionnels de santé aux bonnes pratiques de sécurité, de répartir rôles et responsabilités entre les services biomédicaux et informatiques, d'établir des politiques internes et des procédures opérationnelles pour réduire les risques.

b) Sensibilisation et formation des professionnels

L'instauration d'une culture de sécurité et de démarches d'amélioration continue parmi les personnels d'un établissement permet d'encourager la vigilance et de responsabiliser chacun. Cependant, les démarches qui visent à améliorer la compréhension des risques et l'importance de la sécurité numérique dans les établissements de santé n'émergent que

depuis quelques années et impliquent des efforts nourris de la part de tous les acteurs pour être efficaces.

Le *Guide d'hygiène informatique* de l'ANSSI intitulé *Renforcer la sécurité de son système d'information en 42 mesures* comporte de nombreux conseils mais qui sont plus à destination de la direction des services informatiques.

Introduit à la fin de l'année 2022, le label régional NOUVEY, élaboré en collaboration avec l'ARS et le Groupement de Coopération Sanitaire (**GCS**) Tesis, vise à améliorer la sensibilisation des acteurs de santé en matière de cybersécurité, inciter l'ensemble des professionnels à adopter les bonnes pratiques (Figure 12) et illustrer la dynamique en cours dans le domaine médical et médico-social en matière de cybersécurité, à travers le message suivant : "En informatique comme en médecine, il y a des règles d'hygiène à respecter !" [32] Cette initiative, dont le nom signifie "on veille" en créole, se fixe pour mission de sensibiliser les acteurs de santé aux risques liés à des comportements tels que les clics sur des mails frauduleux, l'usage personnel d'outils professionnels, ou l'utilisation de mots de passe partagés et facilement déchiffrables sont clairement identifiés.

Figure 12 : Campagne de sensibilisation aux risques cyber en santé initiée par le label régional NOUVEY (Source : [33])

DOI : https://doi.org/10.34746/ids213

Entre fin 2022 et début 2023, une campagne de communication éducative a été initiée pour informer et sensibiliser les acteurs de santé aux sujets du label NOUVEY. Cette campagne a employé divers moyens, tels que des affiches (Figure 13), des campagnes sur les réseaux sociaux, des vidéos, des quiz et des infographies. Un site internet dédié a été mis en place pour centraliser les informations. Enfin, des sessions de formations et de sensibilisation, sous forme de webinaires, ont été organisées, et un événement annuel spécifique a été instauré dans le cadre de cette initiative.

Figure 13 : Campagne de sensibilisation aux risques cyber en santé initiée par le label régional NOUVEY (Source : [32])

Le but des différentes actions de sensibilisation engagées sur tout le territoire Français est de faire prendre conscience que les utilisateurs et les acheteurs sont aussi responsables de la bonne gestion des risques cyber pour garantir la sécurité des patients pris en charge dans les établissements de santé et également la confidentialité des données. Le service biomédical a donc un rôle prépondérant dans cette prise de conscience pour pouvoir adopter les bonnes pratiques et les actions nécessaires pour faire face à ces risques cyber.

c) Collaboration entre les services informatiques, médicaux et administratifs pour assurer une approche cohérente et intégrée de la sécurité informatique

Historiquement, les fonctions de support informatique et biomédical étaient délimitées en fonction de l'infrastructure : le service biomédical gérait les dispositifs médicaux tandis que le service informatique était chargé des ordinateurs, serveurs et équipements réseau.
Cependant, la gestion des données biomédicales exige désormais une collaboration plus étroite entre les services informatiques et biomédicaux. Selon l'**AFIB** (Association Française des Ingénieurs Biomédicaux), il est nécessaire de fusionner leurs compétences et de les appliquer conjointement à un domaine d'intérêt commun [34]. Cette fusion est d'autant plus importante qu'un des enjeux majeurs dans la thématique de la cybersécurité est l'opposition

de la vision du Responsable de la Sécurité des Systèmes d'Information (**RSSI**) et du responsable biomédical à propos des équipements biomédicaux (Figure 14). Effectivement, le premier, chargé de définir la politique de sécurité des systèmes d'information et qui veille à son application, souhaite souvent limiter les connexions pour garantir la sécurité des appareils et la confidentialité des données alors que le dernier souhaite l'ouverture et la connexion des **DM** pour faciliter leur utilisation et leurs sauvegardes. Il y a donc un enjeu majeur de dialogue entre les deux services qui doit notamment être facilité par le comité de gestion de la sécurité numérique désormais mis en place dans une grande majorité d'établissements de santé. L'objectif est finalement de trouver un compromis entre les règles de sécurité maximum et les fonctionnalités de travail nécessaires au personnel soignant. De plus, les ingénieurs biomédicaux doivent affirmer que la sécurité numérique des équipements est au cœur de leurs préoccupations et le faire clairement savoir aux fournisseurs [31].

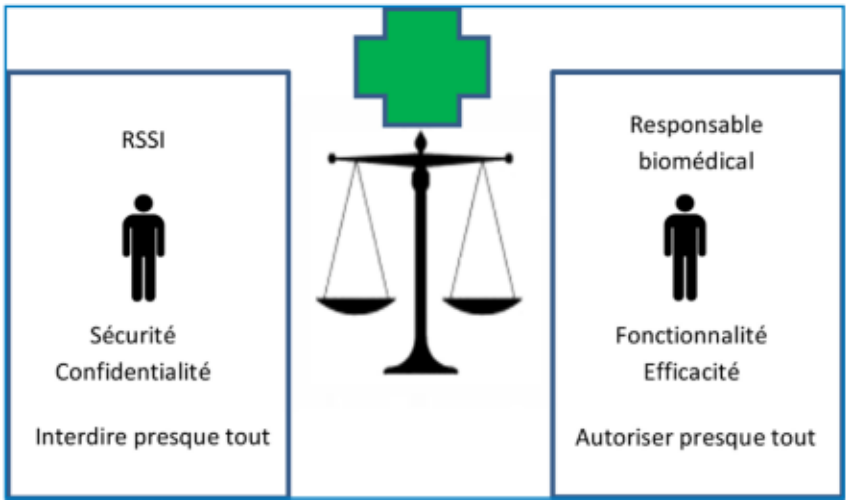


Figure 14 : Différences de visions entre le RSSI et le responsable biomédical à propos des équipements connectés (Source : [31])

Ainsi la gestion de la cybersécurité en termes de moyens, de stratégie et de solutions techniques doit se faire à l'échelle de chaque structure sanitaire et médico-sociale et mobiliser un nombre important et divers d'acteurs.

Les missions des acteurs de la sécurité informatique à l'hôpital commencent d'ores et déjà à évoluer [31].
Parmi eux, on retrouve le **RSSI** qui est également chargé de donner des conseils, une assistance et d'assurer la formation, dont la prévention ainsi qu'un travail de veille à la fois technologique mais également réglementaire. Il doit notamment accompagner le service biomédical dans ses missions. Ensuite il y a les référents technologiques de chaque domaine du système d'information en santé et qui sont les interlocuteurs privilégiés du **RSSI**. Puis la direction des systèmes d'information doit jouer le rôle de facilitateur et d'architecte des solutions informatiques. Enfin, face à la numérisation de l'hôpital, l'ingénieur biomédical a un rôle de plus en plus crucial dans la sécurité. Tous ces acteurs doivent donc collaborer le mieux possible et il s'agit d'un des enjeux majeurs.

Actuellement de plus en plus d'établissements opèrent une réorganisation avec la fusion du service biomédical et de la Direction des Service Informatiques (**DSI**). À mesure que la technicité des **DM** augmente, englobant de nombreuses composantes informatiques et communicantes, les responsabilités des **DSI** et des services biomédicaux se chevauchent. A titre d'exemple, l'expérience réussie au sein du Groupements hospitaliers de territoires (**GHT**) Nord Saône et Loire Bresse Morvan a abouti à une gouvernance partagée entre la **DSI** et le biomédical [35]. Cette approche a permis une réorganisation efficace des espaces, une centralisation des accès, et la mise en place d'un socle informatique solide. Sa conformité aux directives du Ségur du numérique, a amélioré la gestion des activités en cas de dysfonctionnement, renforçant les liens avec la ville, et garantissant la disponibilité des données sur tout le territoire. Au Centre Hospitalier d'Aix-en-Provence, la **DSI** a été chargée d'englober le biomédical, mais des obstacles liés à l'autonomie et au soutien de la direction ont rendu le projet complexe [35].

Ainsi, bien que le rapprochement entre le biomédical et la **DSI** semble être une évolution incontournable à long terme, sa réussite dépendra d'une fusion soutenue par les différents collaborateurs, d'une culture partagée, d'une trajectoire commune, et de l'engagement de la direction générale. L'intérêt d'une telle fusion n'est cependant pas partagé et seul le temps montrera le modèle le plus robuste, fusion ou non.

1.5.3) Mesures juridiques

Les mesures juridiques de la cybersécurité consistent en la mise en place des dispositifs légaux et réglementaires pour protéger les Systèmes d'Information (**SI**), protéger les données médicales sensibles, garantir la continuité des soins, et prévenir les cyberattaques. Cela implique le respect des règlements européens sur les Dispositifs Médicaux (2017/745 et 2017/746) et la protection des Données Personnelles, ainsi que les lois françaises telle que la directive SG/DSSIS/2016/309. Ces différents règlements émettent des exigences sur la protection des données et la définition des responsabilités en cas d'incidents.

a) Règlements Européens

- Règlement Général sur la Protection des Données (RGPD) n°2016/679

Le but de ce règlement est d'informer les patients et les professionnels de leurs droits en matière de gestion des données à caractère personnel et de garantir leur confidentialité. Dans ce cadre, il faut nommer un Délégué à la Protection des Données (**DPO**). Le service biomédical assure donc les missions d'identifier les **DM** produisant des données personnelles, de comprendre les risques liés au SI, aux flux de données et à la nature des données lors de l'achat. Il est également chargé d'annexer le contrat **RGPD** au contrat de maintenance en impliquant le **DPO**, s'assurer de la destruction des données lors de l'élimination des **DM** et enfin signaler au **DPO** tout problème de confidentialité constaté en exploitation des **DM**.

- Règlements européens 2017/745 et 2017/746 relatifs aux dispositifs médicaux et dispositifs médicaux de diagnostic *in vitro*

Ils imposent des exigences spécifiques en matière de sécurité et de performance pour les **DM**, et les articles 14.2.d, 17.4. et 6.1.b du règlement 2017/745 introduisent le concept de **DM** numérique. Ces mesures doivent être appliquées dès la phase de conception des **DM** et être intégrées aux spécifications des produits pour garantir leur utilisation sécurisée dans le domaine médical.

Bien que ces nouveaux règlements permettent de faire entrer certains logiciels et **SI** dans le champ des **DM** et d'augmenter les exigences liées aux risques numériques et aux mises à jour, peu d'articles abordent spécifiquement le lien entre **DM** et cybersécurité.

Parmi les articles qui abordent cette thématique, on retrouve l'article 14.5 qui stipule que les dispositifs destinés à être utilisés avec d'autres dispositifs ou produits doivent être conçus et fabriqués de manière à garantir une interopérabilité et une compatibilité fiables et sécurisées. Cependant, aucune norme requise pour l'obtention du marquage CE, en vue de la mise sur le marché de ces dispositifs, ne traite spécifiquement de l'interopérabilité.
Enfin, l'article 103 du règlement exige la création d'un groupe de coordination européen des **DM**, qui a élaboré en 2019 un guide destiné aux fabricants concernant la cybersécurité des **DM**. Il est important de noter que ce guide n'a cependant pas de valeur légale contraignante et ne renseigne pas l'ingénieur biomédical sur les exigences qu'il doit appliquer.

Il est également important d'évoquer la matériovigilance, régie par ces Règlements européens. En effet, ce champ est crucial pour assurer la sécurité des produits médicaux sur le marché. Ces règlements imposent aux fabricants la mise en place de systèmes de matériovigilance, englobant la collecte, l'évaluation, et le signalement des incidents graves et des effets indésirables. Tant pour les dispositifs médicaux que pour les dispositifs médicaux de diagnostic in vitro, le signalement aux autorités compétentes et aux organisations concernées en cas d'incident majeur est une obligation essentielle. L'objectif principal est d'assurer une surveillance systématique et efficace, ainsi que la prise de mesures correctives appropriées pour garantir la sécurité des patients et des utilisateurs.

- Directive *Network and Information System Security* (***NIS***)

Cette directive, entrée en vigueur en 2023, vise à assurer un niveau de sécurité élevé commun aux réseaux et **SI** de l'Union européenne et à mettre en place des actions face aux risques de cyberattaques [36]. Les 4 enjeux sont les suivants : mettre en place une stratégie nationale de sécurité numérique coordonnée par l'**ANSSI**, de même que la coopération entre les États de l'Union Européenne, renforcer la cybersécurité des opérateurs de service essentiels (**OSE**) et renforcer la cybersécurité des fournisseurs de service numérique.

- Recommandations de l'Agence Nationale de Sécurité du Médicament et des produits de santé :

Le guide *Cybersécurité des DM intégrant du logiciel au cours de leur cycle de vie* indique que les fabricants doivent respecter le **RGPD** et réaliser une analyse des risques des **DM** liée à la cybersécurité. Il donne la manière dont les fournisseurs peuvent atteindre un niveau de risque acceptable mais pas comment les ingénieurs biomédicaux vont pouvoir juger l'acceptabilité du risque.

b) Lois françaises

S'agissant de sécurité, en France, le respect de référentiels est une exigence entrée dans le Code de la Santé Publique. Le Code de la Santé Publique regroupe l'ensemble des dispositions législatives et réglementaires qui encadrent le système de santé en France. Il évolue au fil du temps pour s'adapter aux enjeux contemporains, y compris ceux liés à la sécurité des systèmes d'information dans le domaine de la santé. Les établissements de santé sont tenus de se conformer à ces référentiels de sécurité, et des audits peuvent être réalisés pour vérifier la conformité de leurs pratiques. Les sanctions en cas de non-respect de ces obligations peuvent inclure des amendes et d'autres mesures coercitives, soulignant l'importance de la sécurité des données de santé dans le contexte légal français.

Une des principales lois françaises concernant la cybersécurité est la directive SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information dans les établissements de santé. Cette directive concerne la mise en œuvre du Plan d'action sur la sécurité des systèmes d'information (**SSI**) dans les établissements de santé. Ce plan vise à renforcer la sécurité des systèmes d'information au sein des différents services d'un établissement. Les détails spécifiques de cette instruction incluent des directives sur les mesures de sécurité à mettre en place, les protocoles à suivre et les responsabilités assignées aux établissements et services concernés. En résumé, l'instruction fournit un cadre pour renforcer la protection des systèmes d'information dans le contexte des établissements visés par cette réglementation.
Par conséquent, en cas d'incidents, la mise en œuvre de procédures légales, telles que des enquêtes ou des poursuites judiciaires, contribue à dissuader les attaquants potentiels. Les sanctions prévues par la loi peuvent constituer un élément dissuasif efficace pour les individus ou les organisations cherchant à compromettre la sécurité des systèmes et des établissements. Il est cependant nécessaire de rappeler que la mise en place de ces lois et de sanctions associées en cas de non-respect, ne représente pas réellement un frein pour les cyber attaquants.

Le Gouvernement français se mobilise également pour instaurer des mesures visant à renforcer la sécurité de l'espace numérique. À travers le projet de loi intitulé « Sécuriser et réguler l'espace numérique », l'objectif premier est d'offrir une protection accrue aux citoyens français et aux entreprises, en tenant compte des enjeux sociaux et économiques liés au numérique. Dans un contexte où la France aspire à jouer un rôle prépondérant dans la régulation digitale en Europe, le gouvernement ambitionne de créer un cadre propice à la confiance dans l'environnement numérique. Ce projet de loi vise à établir un ordre public en

ligne, interdisant les activités qui ne sont pas autorisées dans la vie réelle pour garantir la cybersécurité des activités quotidiennes des Français [37]. En ce qui concerne le volet lié au cloud, les députés ont intégré un nouvel article 10 bis A, imposant à l'État et à ses opérateurs l'obligation de faire appel à des entreprises européennes pour l'hébergement des données stratégiques et sensibles. Par ailleurs, des précisions supplémentaires ont été apportées concernant les obligations spécifiques des hébergeurs de données de santé.

c) Limites des mesures juridiques liant la cybersécurité et les dispositifs médicaux

Les enjeux réglementaires de la cybersécurité à l'hôpital sont donc cruciaux et visent à garantir la protection des données médicales sensibles, la continuité des soins, et la prévention des cyberattaques. Il est donc important d'avoir une vision globale des différents règlements, directives et bonnes pratiques les plus pertinentes et comprendre les enjeux qui gravitent autour de la cybersécurité. Cet enjeu est d'autant plus important que le corpus réglementaire autour des DM et des SI demeure restreint. En effet, contrairement aux risques physiques (électronique, mécanique, magnétique, etc..), les risques et contraintes numériques sont peu abordés dans les règlements européens 2017/745 et 2017/746 relatifs aux dispositifs médicaux [34]. Bien que ces nouveaux règlements permettent de faire entrer certains logiciels et SI dans le champ des DM et d'augmenter les exigences liées aux risques numériques et aux mises à jour, peu d'articles abordent spécifiquement le lien entre DM et cybersécurité.

1.6) Apports des travaux de l'Association Française des Ingénieurs Biomédicaux en matière de Sécurité Numérique des équipements biomédicaux

L'ingénieur biomédical possède plusieurs missions en lien avec la cybersécurité mais qui ne sont pas toujours faciles à mettre en place sur le terrain. Comme explicité dans les sections précédentes, il existe des conseils donnés par différentes entités comme l'**ANSSI** ou l'**ANS** mais assez peu d'outils utilisables directement dans les missions quotidiennes des services biomédicaux.

Dans le cadre de ce projet, plusieurs documents et guides abordant la cybersécurité dans le monde de la santé ont été examinés. 75% des documents étaient destinés à l'ensemble des services de l'établissement de santé, 15% concernaient le système informatique et 10% concernaient le service biomédical. Une certaine hétérogénéité des publics cibles peut être constatée de même qu'un faible nombre de recommandations spécifiques aux services biomédicaux, et assez peu d'outils utilisables alors même que le service biomédical a un rôle prépondérant dans la prévention des cyberattaques.

L'**AFIB** a mené un groupe de travail entre 2019 et 2020 visant à étudier l'impact de la réglementation européenne en matière de **DM** sur les missions de l'ingénieur biomédical

dont la prise en compte de la sécurité numérique dans toutes les étapes du cycle de vie des équipements biomédicaux. A l'issue des travaux, une série de recommandations sur la sécurité numérique des équipements biomédicaux a été publiée par l'**AFIB** (Figure 15) [31].

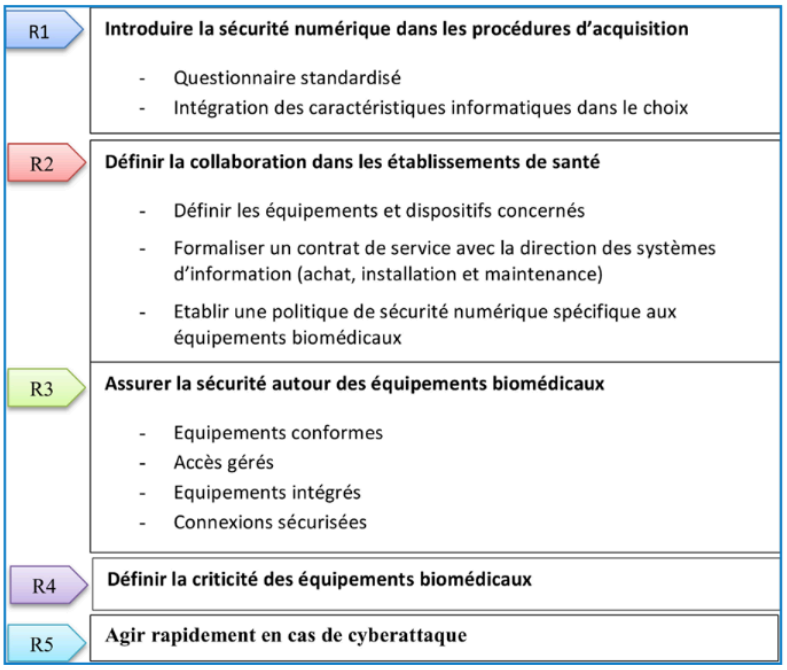


Figure 15 : Tableau des 5 recommandations de l'AFIB pour une meilleure prise en compte des systèmes d'information associés aux équipements biomédicaux (Source : [31])

La première recommandation concerne l'introduction de la sécurité numérique dans les procédures d'acquisition. Le but est d'intégrer la sécurité numérique dès les étapes d'acquisition en utilisant un questionnaire standardisé qui aborde les aspects informatiques et de sécurité numérique. L'objectif est d'augmenter les exigences imposées aux fournisseurs en généralisant ce questionnaire à tous.

En ce qui concerne la collaboration au sein des établissements, l'**AFIB** insiste sur la nécessité d'établir des recommandations concernant la collaboration entre le service biomédical et le service informatique. Les principaux enjeux incluent la définition des responsabilités et des modalités de collaboration, ainsi que l'identification et la gestion des logiciels.

A propos de la sécurité des équipements, les ingénieurs biomédicaux ont pour mission de sécuriser les accès et de vérifier l'intégrité des **DM**. Il est également nécessaire d'élaborer une cartographie détaillée et de participer à une plus grande sensibilisation des utilisateurs aux risques cybers des **DM**.

Dans la quatrième recommandation, il est mention de la définition de la criticité des équipements médicaux et donc la réalisation d'une cartographie des risques associée à des plans d'actions adaptés à ces risques.

Enfin, pour la réponse rapide en cas de cyberattaque, il s'agit de fournir des recommandations visant à permettre une réaction rapide en cas de cyberattaque. Cette recommandation s'appuie sur les directives émises par le ministère de la Santé en réponse à un Message d'Alerte Rapide Sanitaire (**MARS**).

Ainsi 80% des recommandations émises par l'**AFIB** concernent la prévention des cyberattaques dont la démarche est généralisable entre les différents établissements (Figure 16) et ce pour plusieurs raisons. Tout d'abord, au niveau des recommandations de l'**AFIB**, la prévention représente.

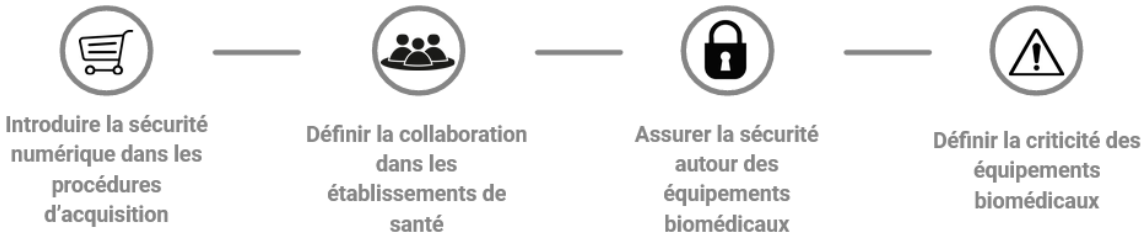


Figure 16 : Schéma des recommandations de l'AFIB concernant la prévention pour une meilleure prise en compte des systèmes d'information associés aux équipements biomédicaux (Source : Auteurs)

Mais des outils concrets facilitant leur mise en application restent à concevoir. La problématique adressée par le présent mémoire est donc la suivante :

Comment outiller les ingénieurs biomédicaux pour mettre en place et améliorer la prévention des cyberattaques au sein des établissements de santé français en se basant sur les recommandations de l'AFIB et sur des retours d'expériences ?

II- Création d'outils à partir des recommandations de l'Association Française des Ingénieurs Biomédicaux

2.1) État des lieux des pratiques biomédicales concernant les risques cyber

Deux questionnaires ont donc été réalisés. Le premier questionnaire était construit en trois parties distinctes. La première partie, qui est celle d'intérêt dans cette section, se concentrait sur les pratiques globales des établissements de santé en matière de cybersécurité (Figure 17) et seront détaillées dans cette section.

Questionnaire	Nature des Données recueillies	Type de Données
Questionnaire 1 (1ère partie)	Information professionnelle des participants	Position occupée dans l'établissement de santé
	Informations sur les outils et méthodes utilisés pour les cyberattaques	Types et description des outils et des méthodes ainsi que leur efficacité et suffisance
	Opinion et retours sur le questionnaire d'introduction de la sécurité numérique dans les achats (Outil 1)	Données qualitatives (opinions, retours, commentaires)

Figure 17 : Tableau récapitulatif de la nature et du type de données recueillies dans le premier questionnaire concernant les pratiques globales des établissements de santé en matière de cybersécurité

La répartition des 75 personnels sollicités, tous formés dans le domaine biomédical, est indiquée en figure 18 selon leur structure d'exercice.

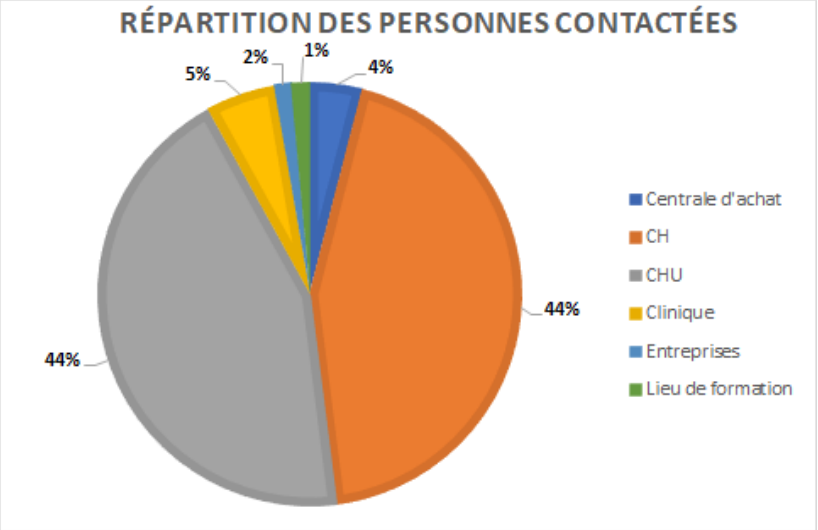


Figure 18 : Répartition des personnes contactées par structure d'appartenance (Source : Auteurs)

Parmi les 75 sollicitations envoyées, 6 réponses ont été obtenues à nos questionnaires après deux relances. La moitié des répondants sont des ingénieurs biomédicaux et l'autre moitié des responsables d'atelier biomédical/techniciens travaillant majoritairement dans des **CHU** (Centres Hospitaliers Universitaires). Le faible nombre de réponses peut s'expliquer par la courte durée du projet ainsi que par le manque de temps des ingénieurs biomédicaux pour répondre à ce type de sollicitations comme expliqué dans la partie limitation de ce mémoire.

En plus des réponses au questionnaire, 8 entretiens ont été menés à la fois pour obtenir des avis sur les outils réalisés mais également pour avoir une idée des missions et du quotidien des services biomédicaux en rapport avec la cybersécurité. La majorité des personnes interrogées sont des ingénieurs biomédicaux (Figure 19) et travaillent dans des Centres Hospitaliers Universitaires (**CHU**)

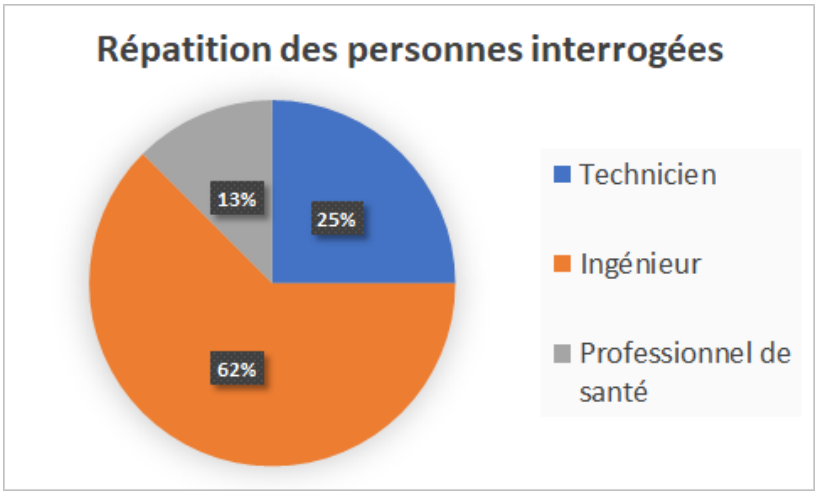


Figure 19 : Répartition des personnes interrogées par fonction (Source : Auteurs)

Les entretiens menés permettent de croiser les visions complémentaires de différents types d'acteurs selon leur fonction et la taille de leur établissement d'appartenance.
A la question, "vous sentez-vous prêt à faire face à une cyberattaque ?", les réponses sont assez convergentes. 50% des répondants ne se sentent pas vraiment prêts, 16,7% pas du tout prêts et 33,3% des répondants ont répondu qu'ils se sentent partiellement prêts (Figure 20). Ce sentiment de manque de préparation face aux risques de cyberattaques ressort également dans les entretiens.

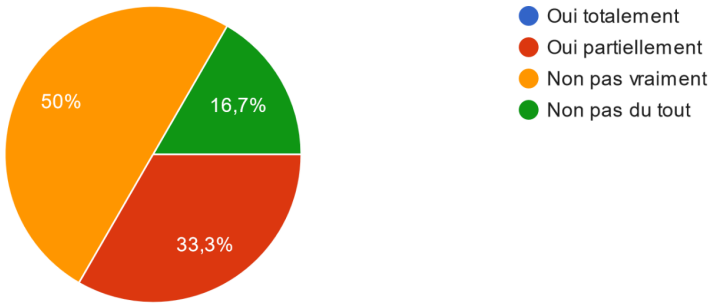


Figure 20 : Réponses à la question : Vous sentez-vous prêts à faire face à une cyberattaque (Source : Auteurs)

La partie générale du questionnaire s'est ensuite concentrée sur les principaux outils et méthodes utilisés par les services biomédicaux pour prévenir les cyberattaques. Les principales pratiques qui ont été remontées, classées par fréquence de retour, sont les suivantes :

- Recensement de tous les DM générant de la donnée sur le réseau et regroupement de ces DM sur un même ***Virtual Local Area Network*** **(VLAN)** pour les isoler du réseau en cas d'attaque ou de coupure réseau.
- Travail en étroite collaboration avec le service informatique et grande confiance dans le travail du service informatique qui participe souvent aux commissions d'achats des DM pour anticiper les modalités de connexion au réseau de l'hôpital
- Mises à jour des OS
- Utilisation d'antivirus et de bastion de sécurité.

Dans 66,7% des cas, ces outils étaient considérés comme efficaces. En effet, la plupart des services s'appuient sur des **VLAN** isolés et donc sécurisés. Si ce switch est déconnecté du réseau, les DM seront autonomes pour ceux qui le peuvent comme les centrales de surveillance et de monitorage. La confiance portée au service informatique, qui a une part importante dans la sécurité des **DM**, contribue également à cette majorité des avis.

Il est à noter que les personnes ayant répondu que leurs outils sont suffisants sont des professionnels du service biomédical qui délèguent une grande partie de la gestion de la cybersécurité à la **DSI**. Certains entretiens mettent en évidence l'hétérogénéité des compétences informatiques dans les services biomédicaux en fonction des établissements. Certains services biomédicaux ayant des compétences suffisantes participent aux missions de cybersécurité alors que d'autres délèguent cette partie à la **DSI**.

Mais les craintes des personnels biomédicaux persistent. Il a par exemple été mentionné que tous les établissements hospitaliers de France et d'ailleurs sont attaqués tous les jours. Un interlocuteur a même cité un dysfonctionnement total de leur supervision sur leur service de stérilisation peu de temps avant le remplissage du questionnaire. Près de 67% des répondants estiment que leurs outils ne sont pas suffisants pour prévenir les cyberattaques : Un anti-virus ne peut pas tout bloquer, certains répondants signalent le peu de mise à jour des logiciels et des Systèmes d'Exploitation (**OS**) ainsi qu'un manque de sensibilisation de tous les professionnels de santé aux risques liés aux **DM** spécifiquement.
Un autre constat est que l'utilisation des VLAN est de plus en plus complexe du fait de l'interconnexion des **DM** avec d'autres logiciels et notamment du fait des flux de données vers le Dossier Patient Informatisé (**DPI**). Pouvoir isoler l'environnement informatique du service de soins est une solution seulement si celui-ci n'a pas l'utilité de communiquer avec l'extérieur.

Le service biomédical gagnerait à monter en compétences en informatique générale et le service informatique en gestion des risques cyber intrinsèques aux DM. Il s'agit effectivement d'une problématique majeure au vu des réponses qui font part de cyberattaques récentes et au fait que 83% des participants disent réaliser des réunions au sein de leur service à propos des problématiques de cybersécurité.

Les échanges avec les professionnels de santé font émerger le manque de solutions concrètes et de supports liés aux risques cyber à destination des ingénieurs biomédicaux qui croulent sous le travail. Les problèmes majeurs semblent être la difficulté de la collaboration entre service biomédical et informatique lors de l'achat d'un dispositif médical ainsi que le manque de procédures dégradées du fait d'un manque d'analyse des risques des dispositifs médicaux. Les recommandations proposées par l'**AFIB** correspondent aux attentes terrains dans leur formulation mais les solutions proposées ne sont pas sous la forme d'outils exploitables. Dans le cadre de ce projet, il a donc été décidé que des outils concrets et adaptés aux besoins des ingénieurs biomédicaux devraient être proposés. Dans chacune des sous-parties les attentes des répondants seront détaillées.

2.2) Introduire la sécurité numérique dans les procédures d'achats

Les procédures d'achats sont centrales dans les missions de l'ingénieur biomédical mais aucun référentiel n'est adopté par tous les établissements de santé comme en témoignent les différents entretiens. Face à ce manque d'harmonisation, la cybersécurité n'est pas plus que ça prise en compte dans le processus d'achat par l'ingénieur biomédical ce qui complique également la tâche pour les fournisseurs de **DM** qui ne comprennent pas nécessairement les attentes des établissements de santé en termes de cybersécurité. Il s'agit donc de fournir un outil simple d'utilisation regroupant les différentes questions en lien avec la sécurité numérique validées par des experts en cybersécurité. Il y a de nombreuses

attentes pour que cet outil soit utilisable à la fois par les fournisseurs, les services biomédical et informatique.

Dans ce sens, l'**AFIB** a proposé un questionnaire standardisé portant sur les questions d'informatique et de sécurité numérique des **DM** et qui a pour objectif de mieux prendre en compte la cybersécurité dans les choix d'achats. Les objectifs visés par l'**AFIB** sont de généraliser un même questionnaire afin de sensibiliser tous les acteurs à la sécurité informatique et faciliter le travail lors des procédures d'achats. Ce questionnaire standardisé vise à aider les professionnels de santé dans la gestion du risque cyber tout au long du cycle d'achat des équipements biomédicaux (Figure 21).

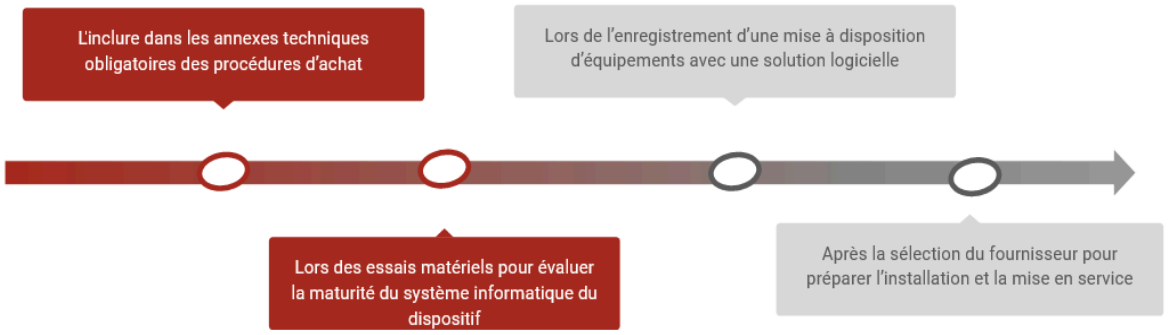


Figure 21 : Schématisation de l'utilisation du questionnaire standardisé de l'AFIB dans le cycle d'achat des équipements biomédicaux (Source : Auteurs)

Il est cependant important de prendre en compte que l'utilisation de ce questionnaire implique une collaboration étroite entre le service biomédical, le service informatique (RSSI notamment) et les utilisateurs pour définir les besoins. En effet, d'après l'**AFIB** : "certaines contraintes doivent être prises en compte en amont de l'achat de tout dispositif médical pour prévenir le manque de sécurité informatique"[31]. Les contraintes majeures sont donc les suivantes :

- Choisir entre les ordinateurs et les serveurs fournis par les fournisseurs ou ceux gérés par le service informatique.
- Indiquer comment les données doivent circuler entre l'équipement et d'autres logiciels de l'établissement.
- Définir les règles internes pour l'accès aux ordinateurs lors de la maintenance à distance.
- Établir les règles de l'établissement pour gérer les accès de tous les utilisateurs

La prise en compte des réponses au questionnaire informatique doit influencer l'évaluation, la sélection de l'équipement et son installation, mais elle n'est pas un critère de blocage. Il est recommandé d'inclure le service informatique dans le processus d'analyse pour évaluer la faisabilité. Cela leur permet de planifier en amont les ressources techniques et financières nécessaires à l'installation.

Ce questionnaire permet donc de prendre en compte les enjeux cybers dès l'achat et de faciliter la collaboration entre service biomédical et informatique pour leur faire gagner du temps à travers une communication facilitée par le biais de questions précises. Cependant, les premiers retours terrains pour ce projet ont mis en lumière que ce questionnaire n'est pas toujours connu et qu'il est difficile d'évoluer dans les centaines de questions qu'il comprend. Un outil interactif pour naviguer entre les différentes questions a été élaboré. Des logigrammes ont été réalisés pour aider l'homme du métier à produire un questionnaire spécifiquement destiné aux fournisseurs (Figure 22).

INFORMATIONS SUR L'EQUIPEMENT
Désignation
Marque
Type
Fabricant et Lieu de fabrication
Fournisseur
Date de première mise sur le marché
Classe du dispositif (I, IIa, IIb, III, DIV) au titre du marquage CE 93/42 ou CE 98/79
Joindre le certificat de conformité CE précisant la classe
Classe du dispositif (I, IIa, IIb, III, DIV) au titre du règlement UE 2017/745 ou 2017/746
Joindre le certificat de conformité CE précisant la classe
S'agit-il d'un logiciel portant le marquage CE des Dispositifs Médicaux ?

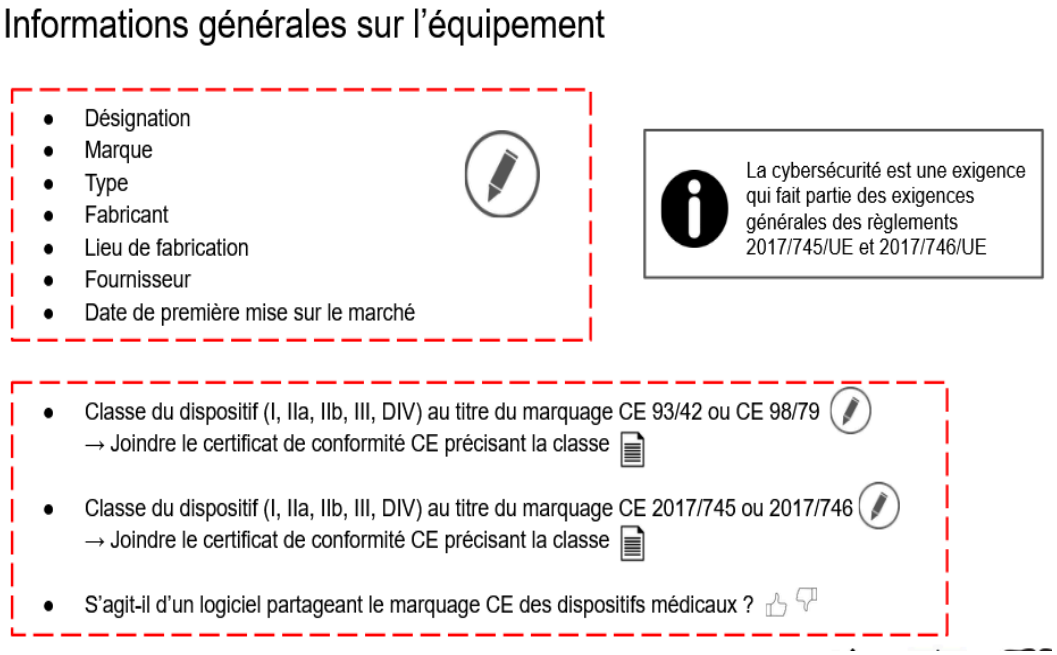


Figure 22 : Comparaison entre les présentations du questionnaire : en haut extraction d'une partie d'une page du questionnaire de la publication de l'AFIB, en bas extraction d'un des logigrammes réalisés pour ce projet (Source : Auteurs)

Le logigramme reprend l'enchaînement de toutes les questions du questionnaire AFIB regroupées en quatre parties, chacune ciblant une caractéristique particulière du dispositif :

- Sa description générale ;
- La description du ou des serveur(s) et une description générique du ou des logiciel(s) ;
- La description du ou des logiciel(s) et leur intégration dans la structure de l'établissement ;
- La description de la maintenance et de la sécurité du ou des logiciel(s).

Pour chacune d'entre elles, une couleur a été assignée pour faciliter le repérage dans la cartographie interactive (Figure 23).

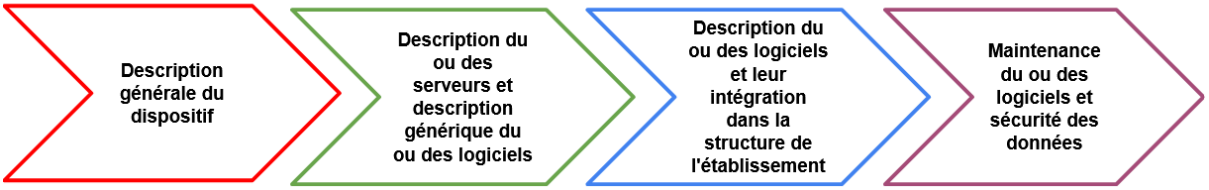
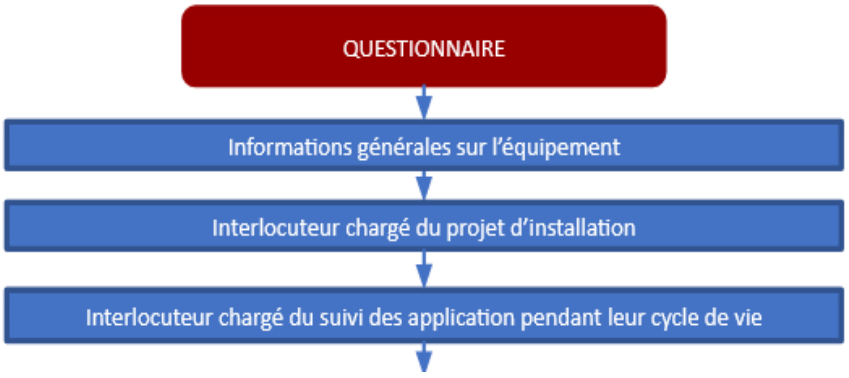


Figure 23 : Les quatre parties de notre questionnaire (Source : Auteurs)

Le logigramme affiche les questions sous forme de blocs. En cliquant sur ces blocs, l'utilisateur peut aller directement aux questions concernées par l'intitulé du bloc, ce qui facilite la lecture du questionnaire ainsi que la navigation entre les différentes questions. Pour chaque bloc, les questions sont listées et un logo indique le type de réponse attendu. Des informations complémentaires pour guider le remplissage et sensibiliser les équipes aux risques cyber sont également données dans les encadrés avec le logo information (Figure 24).



DOI : https://doi.org/10.34746/ids213

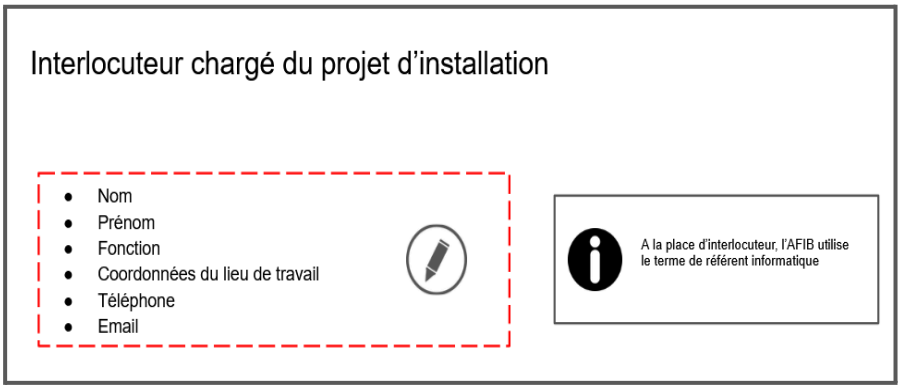


Figure 24 : Présentation d'une partie du logigramme et de la page de question associée à l'interlocuteur chargé du projet d'installation (Source : Auteurs)

2.3) Définir la collaboration dans les établissements de santé

Les retours terrains ont montré que le manque de collaboration entre les services biomédical et informatique freine le déploiement de mesures de prévention des cyberattaques. La difficulté de collaboration s'explique par la répartition des compétences inégale au niveau des logiciels et des postes de travail, le nombre important d'interlocuteurs concernés et l'éventail des diverses expertises requises. En outre, les personnels des services informatique et biomédicaux ont leurs propres missions, budgets et contraintes faisant que la collaboration est souvent perçue comme une surcharge de travail des deux côtés.

A l'heure où les **DM** sont de plus en plus connectés, les compétences informatiques sont devenues obligatoires dans le monde biomédical. Les personnels de tous les établissements ne sont pas encore parfaitement formés aux problématiques de réseau et de cybersécurité en général. C'est pour cela que la collaboration, souhaitable et souhaitée par les personnes interrogées, est cruciale dans les établissements de santé et nécessite d'être accompagnée.

Ainsi, la deuxième recommandation de l'**AFIB** propose un fonctionnement et un partage des compétences et des activités entre personnels biomédicaux et informaticiens basés sur les retours d'expérience de différents établissements. Il s'agit de grandes lignes de conduite favorisant l'instauration du dialogue à adapter au fonctionnement de chaque établissement.

En outre, l'**AFIB** préconise la préparation anticipée d'une stratégie de sécurité numérique spécifique pour les équipements biomédicaux, élaborée en collaboration avec le **RSSI** et le service biomédical [28]. La première démarche consiste ainsi à établir un accord de service entre les services informatique et biomédical, afin de formaliser les attentes mutuelles. Cet accord permettra de définir clairement les attentes et les objectifs de chacun des services impliqués. L'**AFIB** propose trois axes majeurs de travail pour établir cet accord de service :

- Définir le périmètre : Il est essentiel dans un premier temps de déterminer de manière explicite, parmi les logiciels et les postes informatiques, ceux relevant de la compétence et de la responsabilité du service biomédical. Cette évaluation mérite

une révision annuelle pour examiner ce qui a bien fonctionné et ce qui n'a pas fonctionné, permettant ainsi d'ajuster les responsabilités en conséquence.

- Définir les modalités de la collaboration : Il s'agit de répartir clairement les tâches entre le service biomédical et le service informatique afin de ne pas perdre de temps et de mieux anticiper les risques de sécurité numérique.
- Identifier et suivre les logiciels : Chaque application doit faire l'objet d'une fiche d'identification de l'application. Cette fiche doit être conservée par le service concerné afin de gérer l'obsolescence des systèmes d'exploitation et de mieux répartir le suivi et les actions entre services biomédical et informatique.

Les retours terrains indiquent que les personnels des services biomédicaux ne peuvent pas investir le temps nécessaire à la lecture de l'intégralité des recommandations de l'AFIB. Une affiche synthétique en deux pages qui rappelle d'abord pourquoi la collaboration est cruciale puis comment procéder a donc été proposée. Ce format affichette, dont le contenu concerne à la fois le service biomédical et informatique et liste des solutions concrètes combinant les deux points de vue,est plus facile d'accès et s'affiche aisément pour aider les professionnels au quotidien.

La première page de l'affiche repose le contexte de la cybersécurité dans les hôpitaux, et s'axe plus particulièrement sur les **DM**. A l'aide des recommandations de l'**AFIB** et des retours terrain, les différents risques cyber majeurs liés aux **DM** ont été recensés. En effet, les risques généraux liés à la bureautique sont souvent définis dans les documents mais ceux spécifiques aux **DM** ne sont pas ceux les plus mis en avant. En parallèle, le recensement des mauvaises pratiques, qui constituent des risques majeurs pour les cyberattaques, a été effectué. En plus de l'exposition des risques et des mauvaises pratiques, un schéma global d'une cyberattaque typique a été réalisé à partir de données bibliographiques et de retours terrain. Le but recherché n'était pas seulement de formaliser une attaque typique mais également de montrer avec un exemple concret les mauvaises pratiques et erreurs fréquentes et des propositions d'actions à mettre en place pour éviter que la cyberattaque atteigne sa cible. L'objectif de cette affiche est donc de montrer que les services biomédicaux et informatiques, en collaborant, peuvent permettre de réduire les risques cyber et donc de motiver les parties prenantes à réaliser l'accord de service.

La deuxième page de l'affiche se concentre sur les trois axes de travail majeurs pour une collaboration entre services informatique et biomédical définis par l'**AFIB** plus haut. Il s'agit d'expliciter de façon synthétique l'essentiel de la démarche pour donner des pistes d'actions et de répartition des tâches entre les services. L'objectif est donc de servir à la fois de mémo mais également de catalyseur à une meilleure répartition des tâches en donnant à la fois des exemples concrets et des actions adaptées au milieu hospitalier.

2.4) Assurer la sécurité autour des équipements biomédicaux

La troisième recommandation de l'**AFIB** concerne la sécurité des équipements biomédicaux. Ainsi, dans ses recommandations, l'**AFIB** propose 4 axes de travail [31] :

- L'ingénieur biomédical est le garant de la sécurité des équipements biomédicaux : L'ingénieur est en effet responsable de la définition des règles de sécurité spécifiques aux équipements biomédicaux, la conformité au marquage CE, le maintien de la continuité des soins, le signalement des incidents et la réalisation d'audits de sécurité en collaboration avec le **RSSI**.
- Seules les personnes autorisées peuvent utiliser un équipement biomédical : L'ingénieur biomédical gère les droits d'accès, la sécurisation des codes d'accès et le contrôle des accès physiques aux locaux.
- L'intégrité des équipements biomédicaux doit être respectée : L'ingénieur biomédical se doit de gérer le suivi des accessoires et éléments installés, la documentation des changements et la protection des données sensibles liées à l'installation.
- Les connexions et transferts de données doivent être sécurisées : Parmi ses missions, l'ingénieur biomédical gère le blocage des ports d'entrées non utilisés, la restriction des supports mobiles **USB**, la documentation des interfaces de communication, et la segmentation des réseaux d'équipements.

L'ingénieur biomédical a donc de multiples missions, ce qui implique un rôle de sensibilisation des utilisateurs pour garantir la sécurité des **DM** à l'échelle de tout l'établissement de santé. Cependant, d'après les retours terrains, le service biomédical n'est pas très présent dans la réalisation de cette tâche étant donné que d'autres missions apparaissent comme plus prioritaires et c'est bien souvent le service informatique qui s'occupe de la prévention auprès des utilisateurs. Cela semble notamment lié à un manque de temps pour chercher et préparer des ressources concernant spécifiquement les risques cyber liés aux **DM**. Il y a en effet de nombreuses ressources concernant les dangers des mails étant donné que c'est la première cause d'intrusion [38]. Or, le ***phishing*** ne concerne pas directement les **DM** mais plutôt toutes les suites bureautiques qui sont sous la responsabilité du service informatique. cyber

Les périphériques **USB** sont souvent directement connectés aux **DM** pour des mises à jour, des transferts de données ou d'autres opérations [39]. Une infection par un ***malware*** provenant d'un périphérique **USB** peut directement compromettre la sécurité du **DM** et des informations médicales. Ensuite, dans les établissements de santé, les périphériques **USB** sont souvent utilisés fréquemment, et il peut être difficile de contrôler leur utilisation. Par conséquent, il existe une probabilité plus élevée que des logiciels malveillants soient introduits par des périphériques **USB** infectés. Les périphériques **USB** sont de plus en plus bloqués dans les hôpitaux mais ce n'est pas le cas partout. Les retours terrains de quelques soignants ont montré que de nombreux praticiens utilisent tout de même des périphériques **USB** et qu'ils ne sont pas aussi sensibilisés aux risques des clés **USB** comparés aux mails. Il est possible d'émettre l'hypothèse que les politiques de sécurité peuvent être plus difficiles à appliquer sur les périphériques **USB** et que moins d'outils de sensibilisation ont été réalisés que pour les risques liés aux mails. Les employés pourraient être moins conscients des risques associés à leur utilisation, augmentant les chances d'introduire des logiciels malveillants.

Une vidéo de moins de 4 minutes a donc été réalisée se concentrant spécifiquement sur la problématique des **DM** dans l'objectif de fournir un outil rapide aux ingénieurs biomédicaux à diffuser à tous les professionnels de santé. La vidéo se veut la plus simple et ergonomique possible avec de nombreuses images, des explications assez brèves et des exemples spécifiques au milieu hospitalier. Les informations utilisées proviennent principalement de documents produits par l'Etat, des retours terrains et d'expériences professionnelles en tant que stagiaires [40]. Le service biomédical est invité à compléter cette vidéo d'explications plus détaillées concernant leur structure de santé pour maximiser les messages de prévention.

2.5) Définir la criticité des équipements biomédicaux

La quatrième recommandation de l'**AFIB** concerne la définition de la criticité des équipements biomédicaux. Afin de définir cette criticité et d'identifier des actions à mettre en place pour les réduire, l'AFIB rappelle qu'il est nécessaire d'évaluer la vulnérabilité des DM individuellement en utilisant une ou plusieurs échelle(s) de notation. Ainsi l'association recommande de combiner une échelle de criticité et une échelle de vulnérabilité pour déterminer avec le plus de précision possible la gravité du risque associé à l'équipement biomédical [28].
La criticité est définie selon la norme ISO 60812 comme "la combinaison de la sévérité d'un effet et de la fréquence de son apparition, ou d'autres attributs d'une défaillance comme une mesure de la nécessité d'un traitement ou d'une atténuation." [32].

La vulnérabilité d'un réseau ou d'un système d'information est défini par l'**ANSSI** comme : "une faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser" [33].

Les ingénieurs biomédicaux ne réalisent pas de cotation normée des risques de chaque équipement biomédical. Ils réalisent la plupart du temps des analyses pour intégrer les **DM** en limitant les risques cyber et l'introduction de nouvelles menaces dans le réseau. Mais ces analyses des risques sont restreintes dans la mesure où elles n'ont lieu uniquement lors de l'installation d'un nouveau **DM** dont le cycle de vie n'est pas toujours pris en compte. Les ingénieurs biomédicaux manquent donc d'un outil synthétique qui propose une cotation normée des risques avec des critères d'évaluation spécifiques aux risques cyber pertinents

Pour ce faire deux échelles de notations ont été retenues :

- Concernant la criticité des équipements médicaux, le choix s'est porté sur la Méthode d'Analyse de la Criticité des **DM** en Exploitation (**MACE**) [41]. La méthode **MACE** est considérée comme l'une des plus pertinentes pour définir la criticité des équipements biomédicaux pour plusieurs raisons. Tout d'abord, cette méthode est spécialement conçue pour les **DM** et donc prend en compte les caractéristiques uniques de ces équipements, y compris leur impact sur la sécurité des patients et la qualité des soins de santé. De plus, la méthode **MACE** évalue la criticité en prenant en considération divers aspects, tels que la sécurité des patients, l'impact sur les

soins, la disponibilité de l'équipement, l'usage fait de l'équipement et la maintenance notamment. Enfin, les critères étant orientés spécifiquement sur les **DM**, la méthode **MACE** aide les établissements de santé à hiérarchiser leurs efforts en matière de maintenance, de gestion des risques et d'investissements en équipements.

- En ce qui concerne la vulnérabilité, le choix s'est porté sur les 10 critères de vulnérabilités numériques des équipements biomédicaux du groupe de travail de l'**AFIB** 2019-2020 [31]. En effet, l'échelle de cotation permet de pointer les caractéristiques liées au système informatique des **DM** qui constituent une porte d'entrée permettant l'accès aux données personnelles du patient, la modification de ces données, interférer sur le fonctionnement du dispositif médical et/ou de constituer un point d'entrée vers d'autres équipements. Cette notion de vulnérabilité est assez peu abordée dans la littérature et lorsque c'est le cas, les questionnaires ne portent pas spécifiquement sur la thématique du numérique. Ce questionnaire est donc particulièrement pertinent pour cet outil d'analyse des risques.

L'outil vise donc à réaliser une cartographie des risques en combinant les méthodes **MACE** et les 10 points de vulnérabilité afin de déterminer un score qui permettra de se placer dans une matrice plus globale.

Ces trois matrices sont intégrées dans une cartographie interactive. En effet, le but n'est pas seulement de fournir les questions et un score de risque mais également d'expliquer l'intérêt de chacune des questions et de fournir quelques informations complémentaires afin d'aider au remplissage. Enfin, une fois le risque déterminé, pour chacun des 3 niveaux définis (acceptable, modéré, fort), plusieurs solutions sont proposées aux utilisateurs. Ces solutions sont réparties en 9 catégories :

- Référencez-vous suffisamment votre parc informatique ?
- Effectuez-vous des sauvegardes régulièrement ?
- Appliquez-vous régulièrement des mises à jour ?
- Utilisez-vous des dispositifs informatiques afin de sécuriser vos données ?
- Avez-vous implémenté une politique d'usage des mots de passe robustes ?
- Avez-vous une utilisation sûre des outils numériques
- Maîtrisez-vous le risque numérique lié au nomadisme des professionnels ?
- Gérez-vous correctement les relations avec vos collaborateurs et tiers-personnes ?
- Quelles actions mettez-vous en place pour réagir en cas de cyberattaques ?

Ces questions ont été inspirées par le document *La cybersécurité pour le social et le médico-social en 13 questions* produit par l'Agence du Numérique en Santé (**ANS**) [42]. Les réponses apportées sont issues de ce document, des autres lectures citées dans la bibliographie [12, 30, 31, 34], de retours terrains et de retours d'expérience en tant que stagiaires. Les différentes personnes interrogées ont partagé les différents points d'attention dans leur quotidien. On retrouve notamment l'utilisation d'antivirus, de VLAN, une bonne

compréhension de l'architecture réseau de l'établissement ou faire attention aux versions d'**OS**. Chacune des catégories est donc enrichie de ces recommandations.

L'utilisation de cet outil d'analyse des risques fonctionne donc selon un processus en 4 étapes (Figure 25). Pour réaliser une analyse des risques complète pour une catégorie de **DM**, il faut compter entre 5 et 10 minutes.

Figure 25 : Schématisation du processus de notre outil (Source : Auteurs)

Un exemple est également donné à propos d'un moniteur paramétrique (résultat en figure 26) pour expliciter la mise en œuvre du processus en 4 étapes.La première étape est donc de calculer un score de criticité en utilisant la méthode **MACE** qui est ici de 22/36 et donc une criticité modérée. Puis il faut remplir le questionnaire de vulnérabilité qui donne ici un score de 5/10, donnant une vulnérabilité modérée. En plaçant les résultats dans la matrice, le risque est évalué comme modéré ce qui donne accès à 9 critères pour élaborer des plans afin de réduire les risques associés à ce **DM**.

		Niveau de criticité du DM		
		Forte	Modérée	Acceptable
Vulnérabilité numérique du dispositif médical	Forte			
	Modérée		X	
	Acceptable			

Figure 26 : Matrice du niveau de risque cyber associé à un dispositif médical, prenant en compte la vulnérabilité et la criticité de celui-ci (Source : Auteurs)

Cet outil n'est pas utilisable pour chaque équipement déjà présent sur le parc hospitalier par manque de temps et de moyens humains. Il semble donc préférable de réaliser cette analyse dans les cas suivants :

- A l'achat d'une nouvelle catégorie de **DM**
- Par code **CNEH** (Centre National de l'Expertise Hospitalière)
- Par code **EMDN** (Nomenclature européenne des dispositifs médicaux)

Ainsi utilisé, l'outil permet d'établir une cartographie des risques des **DM** et de les classer par ordre de priorité en ce qui concerne les actions de cybersécurité à mettre en place. Les plans d'actions devront donc être réalisés en s'inspirant des 9 catégories proposées plus haut dans ce mémoire.

III- Retours terrain et analyse approfondie des outils de cybersécurité

3.1) Présentation des modalités de recueil des avis sur les 4 outils de cybersécurité

Afin d'améliorer les outils présentés dans le chapitre II et de les rendre pertinents pour la communauté biomédicale, il était nécessaire de soumettre les premières versions aux utilisateurs cibles. La partie III de ce mémoire s'attachera à présenter les différents retours obtenus.
Pour cela, deux questionnaires ont donc été réalisés (Figure 27) :

- Le premier questionnaire était construit en trois parties distinctes comme expliqué précédemment. Les deuxième et troisième parties se concentrent sur les opinions et retours sur le questionnaire d'introduction de la sécurité numérique dans les achats et sur l'analyse des risques.
- Le deuxième formulaire visait à recueillir les avis des professionnels sur la vidéo de sensibilisation et sur la fiche de facilitation de la collaboration.

Questionnaire	Nature des Données recueillies	Type de Données
Questionnaire 1 (2ème et 3ème partie)	Information professionnelle des participants	Position occupée dans l'établissement de santé
	Opinion et retours sur le questionnaire d'introduction de la sécurité numérique dans les achats (Outil 1)	Données qualitatives (opinions, retours, commentaires)
	Opinion et retours sur l'analyse des risques cybers d'un DM (Outil 4)	Données qualitatives (opinions, retours, commentaires)
	Suggestions d'amélioration	Données libres (suggestions)
Questionnaire 2	Information professionnelle des participants	Position occupée dans l'établissement de santé
	Opinion et retours sur la fiche de collaboration entre service biomédical et informatique (Outil 2)	Données qualitatives (opinions, retours, commentaires)
	Opinion et retours sur la vidéo de sensibilisation (Outil 3)	Données qualitatives (opinions, retours, commentaires)
	Suggestions d'amélioration	Données qualitatives (opinions, retours, commentaires)

Figure 27 : Tableau récapitulatif de la nature et du type de données recueillies dans les 2 questionnaires (Source : Auteurs)

3.2) Introduire la sécurité numérique dans les procédures d'achats

La majorité des répondants ont reconnu ne pas connaître le questionnaire standardisé proposé par l'AFIB. Les répondants au fait de l'existence du questionnaire indiquent pour la plupart ne pas l'utiliser dans leurs procédures d'achat. Ce questionnaire, pourtant considéré comme intéressant par la plupart des professionnels, manque donc de visibilité. Les entretiens avec un Technicien biomédical de l'**AP-HP** et un Correspondant Sécurité du Système d'information pour le Biomédical au sein d'un **CHU** montrent cependant que des réflexions sont en cours sur l'intégration de ce questionnaire dans les centrales d'achats et qu'il y a une prise de conscience du fait que la cybersécurité doit être incluse tout au long des processus d'achats. L'outil créé dans le cadre de ce projet pourra donc permettre une plus large diffusion de ce questionnaire et, tout du moins une prise de conscience du fait que des solutions existent et sont déjà utiles et utilisables.

Concernant l'évaluation par les premiers utilisateurs de la cartographie proposée pour naviguer dans le questionnaire standardisé de l'**AFIB**, tous les répondants estiment que l'outil est de prise en main aisée et qu'il est agréable au niveau de sa navigation et de son design. Ainsi, la moitié des participants estiment que cet outil est facile d'utilisation et l'autre moitié qu'il est clair. Près de 16% des participants estiment que l'outil est utilisable en l'état et 84% comptent utiliser cet outil sous réserve d'une appropriation interne et après personnalisation à la politique de leur établissement. Ces résultats démontrent l l'intérêt des professionnels biomédicaux pour cette cartographie interactive, le caractère utile et utilisable de cet outil qui sera vraisemblablement utilisé : plusieurs répondants nous ont indiqué penser à l'intégrer dorénavant dans l'évaluation des achats sous réserve que leur service informatique le apporte son point de vue sur l'outil et le valide.

Une des principales limitations remontées est la nécessité que les sociétés postulant aux appels d'offres répondent de façon explicite à toutes les questions et qu'elles soient satisfaisantes et prouvées par le service informatique de l'établissement. L'utilisation de ce questionnaire nécessite donc une pleine collaboration entre service biomédical et informatique.

Il pourrait donc être intéressant de soumettre ce questionnaire aux professionnels des services informatiques hospitaliers. Cela améliorera le contenu du questionnaire et facilitera sa diffusion.

3.3) Définir la collaboration dans les établissements de santé

Tous les entretiens montrent que la collaboration entre service biomédical et service informatique est d'une importance majeure dans la gestion des risques cyber. Cependant, cette collaboration est loin d'être optimale dans tous les services. Dans certains services, les ingénieurs biomédicaux doivent communiquer avec un nombre important d'interlocuteurs du service informatique. Par exemple un interlocuteur pour la connectivité, un spécialisé dans

l'applicatif, et un autre ayant des compétences dans la sécurité pour mettre en place les accès à distance pour les fournisseurs. Cette diversité d'interlocuteurs et le manque de référents du service informatique, dans certains établissements, pour gérer les projets du biomédical rend la gestion de la cybersécurité plus complexe. La collaboration entre les services intervient cependant à toutes les étapes du cycle de vie du dispositif médical et mérite d'être améliorée.

L'outil produit sous forme d'une affiche a été bien accueilli par les services où la collaboration est en train de se mettre en place mais que le budget ou les tâches ne sont pas assez bien réparties. Cette affiche a été décrite comme résumant bien les enjeux de la collaboration et 2 des ingénieurs interrogés l'avaient déjà imprimée lors des entretiens et comptaient l'afficher et la transmettre à leurs collègues de l'informatique. Le schéma simplifié d'une cyberattaque avec des exemples d'erreurs et de solutions semble être la partie de l'affiche qui a le plus répondu aux attentes des ingénieurs biomédicaux. En effet, ils estimaient que ce schéma était très complet et résumait parfaitement les besoins et les problèmes.

3.4) Assurer la sécurité autour des équipements biomédicaux

Selon les retours du terrain, le service informatique semble davantage impliqué dans des initiatives de sensibilisation par rapport au service biomédical, même si ce dernier est responsable de l'utilisation appropriée des **DM** et de la sécurité autour des équipements biomédicaux [31]. Les deux services préconisent cependant d'éviter l'utilisation des clés USB sur les **DM**, mais les entretiens indiquent qu'il existe peu de solutions de remplacement viables. Ce problème constitue une préoccupation majeure, et une sensibilisation accrue pourrait en effet contribuer à trouver des solutions alternatives. Les questionnaires adressés aux professionnels biomédicaux et de santé révèlent que la problématique des périphériques USB fait l'objet de moins de sensibilisation que les dangers liés aux courriels. Par exemple, il est fréquent que des médecins utilisent des disques durs personnels dans les blocs opératoires pour présenter des images lors de congrès ou les étudier en dehors de l'établissement. Un autre exemple concerne l'utilisation d'une clé USB par un ingénieur d'application sur un échographe neuf pour configurer différentes options. Il est évident que les services informatiques et biomédicaux ont des limites quant à leur capacité à contrôler toutes les pratiques et à bloquer toutes les menaces.

La vidéo a été qualifiée de pédagogique et présente un réel potentiel de sensibilisation car les soignants n'ont pas forcément conscience que sur un **DM** il y a les mêmes risques que chez eux mais avec un impact fort sur le patient en plus.

3.5) Définir la criticité des équipements biomédicaux

L'analyse des risques pour l'ensemble des **DM** dans un établissement de santé se révèle être une tâche complexe et chronophage pour le service biomédical. Selon les entretiens réalisés dans le cadre du projet, il est noté que cette analyse est souvent omise. La majorité

des répondants indiquent n'avoir pas effectué de cartographie des risques informatiques liés à leurs DM. Toutefois, tous reconnaissent que l'outil d'analyse des risques des DM proposé dans le cadre du projet est particulièrement intéressant pour prévenir les cyberattaques et élaborer des plans d'actions. Certains participants soulignent même que cette approche d'analyse des risques apporte une dimension supplémentaire dans le processus de sélection des DM lors de leur mise en concurrence.

Une majorité des participants indique que l'outil est facile à prendre en main et est agréable au niveau de son utilisation globale. Un tiers des participants indique vouloir utiliser cet outil dans leur service dans l'état actuel, la moitié sous réserve d'améliorations dans sa forme (conversion au format Excel), ou d'appropriation, c'est-à-dire plus de temps à y consacrer. Près de 17% des participants ne souhaite pas l'utiliser par manque de temps et de moyens.

Les principales améliorations concernent la personnalisation à la politique de l'établissement et avoir plus de temps à y consacrer pour vraiment être en mesure de l'utiliser. En effet, d'après les retours, cet outil est relativement simple à mettre en place mais il faut prendre le temps d'intégrer ce nouveau critère de criticité. L'analyse des risques par l'outil est perçue comme très pointue au point de freiner sa mise en œuvre. En effet, l'ingénieur biomédical manque de temps pour traiter les sujets en profondeur malgré l'intérêt que présente une telle démarche.

Une conversion de l'outil au format Excel a donc été réalisée pour faciliter sa prise en main, sur la base d'une présentation de l'analyse des risques des achats de **DM** créée au format ppt. La conversion permet de rendre l'analyse des risques plus interactive, là où la présentation se concentre sur l'exposé de la démarche, des notions et des questions de l'approche par les risques. Ainsi, l'outil présente 3 onglets avec lesquels l'utilisateur peut interagir. Le premier onglet présente l'analyse **MACE** et permet d'attribuer un score pour chaque critère que l'analyse prend en compte. Le second onglet permet d'établir un score de vulnérabilité du **DM** et de son environnement dans le SI. Le dernier présente la matrice du risque à l'utilisateur pour lui indiquer son niveau de risque et ensuite le guider dans son amélioration de la diminution du risque lié aux cyberattaques sur ses **DM**.

En plus de la détermination du niveau de risque, l'utilisateur est redirigé vers un onglet rassemblant des recommandations d'actions à mettre en place ou à pérenniser selon le niveau de risque du DM par une série de boutons cliquables présentée en figure 28. Les indications présentées dans l'outil Excel sont, de fait, celles qui sont présentées dans l'outil de présentation de l'analyse des risques utilisant la méthode **MACE**. Il est à noter que l'outil laisse la possibilité à l'utilisateur de consulter les recommandations pour chaque type de risque. Il peut ainsi se renseigner sur d'autres actions qu'il pourrait mettre en place pour améliorer sa gestion des risques liés à la cybermalveillance.

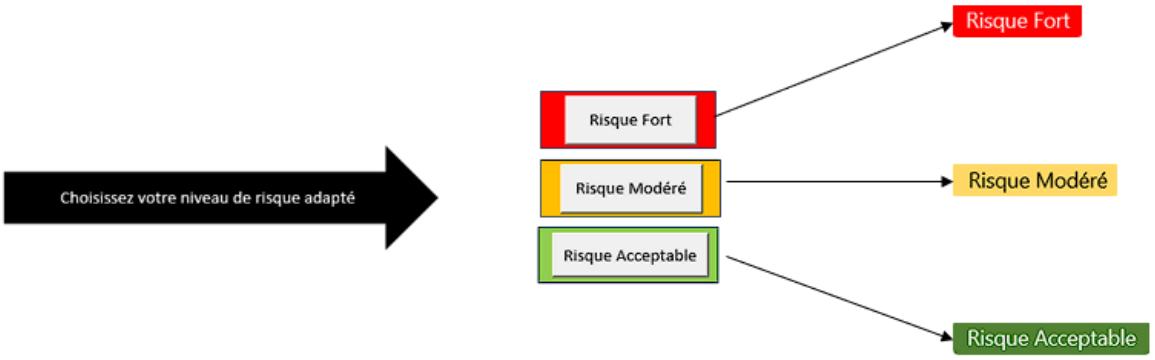


Figure 28 : Boutons de renvoi vers le plan de gestion des risques selon le niveau de risque calculé par l'utilisateur (Source : Auteurs)

Une autre amélioration proposée lors des entretiens est de pré remplir la matrice de risques pour les grandes familles de dispositifs, en suivant par exemple les codes **CNEH** ou **EMDN**. Il s'agirait d'uniformiser les notations entre tous les opérateurs et tous les services biomédicaux et de disposer d'une base commune la plus objective possible, ce qui favoriserait la diffusion de l'outil.

Des futures améliorations consistent en l'intégration des résultats dans la **GMAO** afin de centraliser les informations et aider le service biomédical dans ses prises de décisions.

3.6) Limites des réalisations du projet et pistes d'amélioration

Certaines limitations concernant la méthodologie de ce projet ont été remontées. En effet, dans le recueil des avis de la communauté biomédicale, de nombreux téléchargements ont été constatés, 28 téléchargements sur les 60 mails envoyés mais une faible part de réponses. Cela peut s'expliquer par le fait que tester tous les outils est particulièrement chronophage or les ingénieurs biomédicaux n'ont que peu de temps pour traiter leurs mails. Ces derniers préfèrent partager leurs avis via de courts entretiens plutôt qu'en répondant à des questionnaires. Ce constat peut servir aux prochains étudiants qui vont réaliser des projets dans le cadre de ce Master.

Ensuite, ce projet, de par son large champ d'étude, a permis de proposer des premiers outils à la communauté biomédicale. Afin de vérifier l'utilisation concrète de ces outils sur le terrain, un travail de diffusion ainsi que de recueil des expériences d'utilisation devra se poursuivre par d'autres étudiants du Master Ingénierie de la Santé de l'Université de Technologies de Compiègne pour obtenir des informations détaillées sur la prise en main de ces outils. Ce travail pourrait également être réalisé dans le cadre des travaux de l'**AFIB**.

DOI : https://doi.org/10.34746/ids213

Conclusion

Les cyberattaques dans les établissements de santé, d'incidence croissante, impactent significativement la sécurité et la continuité de la prise en charge des patients ainsi que le budget des établissements. L'ingénieur biomédical, à la croisée de ces nouveaux enjeux, doit être accompagné dans la gestion du risque cyber des dispositifs médicaux.

L'**Association Française des Ingénieurs Biomédicaux (AFIB)** joue un rôle central en proposant des recommandations spécifiques pour renforcer la sécurité numérique des équipements biomédicaux. L'approche proposée par l'AFIB, axée sur l'intégration de la sécurité numérique dans les procédures d'achats, la définition de la collaboration la plus efficace possible entre services informatique et biomédical, l'assurance de la sécurité des équipements, et l'évaluation de la criticité des dispositifs, offre un cadre complet pour armer l'ingénieur biomédical face à ces cybermenaces.

Pour améliorer l'appropriation et la mise en œuvre effective de ces recommandations, des outils spécifiques ont été élaborés avec l'appui de professionnels du service biomédical. Ces outils de cybersécurité adaptés aux besoins des **DM** sont utilisables en l'état et déjà exploités dans certains services. Pour répondre davantage aux attentes de la communauté biomédicale, certaines évolutions ont été proposées, comme standardiser la matrice de risques par famille de DM et intégrer les résultats de l'analyse de criticité des DM à la GMAO, qui pourront faire l'objet de travaux ultérieurs par de futurs étudiants du Master Ingénierie de la Santé de l'Université de Technologie de Compiègne.

Bibliographie

[1] Centre gouvernemental de veille, d'alerte, et de réponse aux attaques informatiques, « À propos du CERT-FR », 2023, [En ligne]. Disponible sur : https://www.cert.ssi.gouv.fr/a-propos/ (consulté le déc. 19, 2023).

[2] Club des Experts de la Sécurité de l'Information et du Numérique, « CESIN », 2023, [En ligne]. Disponible sur : https://cesin.fr (consulté le déc. 19, 2023).

[3] Proofpoint, « Threat reference : répertoire des cybermenaces et attaques internet », mars 2021, [En ligne]. Disponible sur : https://www.proofpoint.com/fr/threat-reference (consulté le déc. 19, 2023).

[4] Agence de l'Union Européenne pour la Cybersécurité, « À propos de l'ENISA», 2023, [En ligne]. Disponible sur : https://www.enisa.europa.eu/about-enisa/about/fr (consulté le déc. 19, 2023).

[5] Futura, « Botnet : qu'est-ce que c'est ? » [En ligne]. Disponible sur : https://www.futura-sciences.com/tech/definitions/internet-botnet-4368/ (consulté le déc. 19, 2023).

[6] Gouvernement, « Cybercriminalité - risques », mai 2022, [En ligne]. Disponible sur : https://www.gouvernement.fr/risques/cyber-criminalite (consulté le déc. 19, 2023).

[7] Kaspersky, « Que sont le deep web et le dark web ? » août 2023, [En ligne]. Disponible sur : https://www.kaspersky.fr/resource-center/threats/deep-web (consulté le déc. 19, 2023).

[8] Ministère de la Santé et de la Prévention, « Système de santé, médico-social et social », 2023, [En ligne]. Disponible sur : https://sante.gouv.fr/systeme-de-sante/systeme-de-sante/article/systeme-de-sante-medico-social-et-social (consulté le déc. 19, 2023).

[9] J. Vance, « Qu'est-ce qu'un vlan et comment fonctionne-t-il ? », Le monde informatique, juin 2022, [En ligne]. Disponible sur : https://www.lemondeinformatique.fr/actualites/lire-qu-est-ce-qu-un-vlan-et-comment-fonctionne-t-il-87023.html (consulté le déc. 19, 2023).

[10] E. Boussin and J. Schreiber, « Retour sur les grandes cyberattaques en France en 2022 : quelles résolutions pour 2023 ? » Portail de l'Intelligence Economique, janvier 2023, [En ligne]. Disponible sur : https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2023/retour-sur-les-grandes-c yberattaques-en-france-en-2022-quelles-resolutions-pour-2023/ (consulté le déc. 19, 2023).

[11] Y. Forest, F. Gama, S. Rasle, O. Declerck, and N. Amani, Webinaire de sensibilisation à la cybersécurité, avril 2022, [En ligne]. Disponible sur : https://www.auvergne-rhone-alpes.ars.sante.fr/cybersecurite-en-etablissement-de-sante-webinaire-replay (consulté le déc. 19, 2023).

[12] V. Branger, B. Louvois, and B. Serre, Guide « Comment se prémunir des cyberattaques ? », Resah-Editions, 2022, [En ligne]. Disponible sur : https://www.resah.fr/centre-de-ressources-et-d-expertise/publications/ (consulté le sept. 20, 2023).

[13] J. Notin, C. Lemal, and M. Derville, « Rapport d'activité sur les chiffres et tendances des cybermenaces : Cybermalveillance.gouv.fr dévoile son rapport d'activité 2021 », mars 2022, [En ligne]. Disponible sur : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2021 (consulté le nov. 3, 2023).

[14] J. Notin, C. Lemal, M. Derville, S. Azzoli, and B. Hervieu, « Rapport d'activité sur les chiffres et tendances des cybermenaces : Cybermalveillance.gouv.fr dévoile son rapport d'ac- tivité 2022 », mars 2023, [En ligne]. Disponible sur : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2022 (consulté le nov. 3, 2023).

[15] Assemblée Nationale, Amendement n°470 du 09/11/2022, Texte n°436, adopté par la Commission sur le projet de loi adopté par le Sénat d'orientation et de programmation du Ministère de l'Intérieur (n°343), novembre 2022, [En ligne]. Disponible sur : https://www.assemblee-nationale.fr/dyn/16/amendements/0436/AN/470 (consulté le sept. 20, 2023).

[16] J. Notin, C. Lemal, and M. Derville, « Retour sur 2021 en infographie », Agence cybermalveillance.gouv, mars 2022, [En ligne]. Disponible sur : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2021 (consulté le nov. 3, 2023).

[17] J. Notin, M. Derville, C. Lemal, S. Azzoli, and B. Hervieu, « Retour sur 2022 en infographie, Agence cybermalveillance.gouv, mars 2023, [En ligne]. Disponible sur : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2022 (consulté le nov. 3, 2023).

[18] NDMN, « Cybersécurité en France, 10 statistiques clés à connaître en 2022 ! », juin 2022, [En ligne]. Disponible sur : https://www.ndnm.fr/statistiques-cybersecurite-2022 (consulté le sept. 20, 2023).

[19] C. Thierache and C. Leroy-Blanvillain, « Cybercriminalité : l'UE présente son projet de règlement « cyber solidarity act » », Alerion Avocats Paris, avril 2023, [En ligne]. Disponible sur : https://www.alerionavocats.com/cybercriminalite-ue-presente-projet-reglement-cyber-solidarity-act/ (consulté le dec. 6, 2023).

[20] Agence nationale de la sécurité des systèmes d'information, Rapport « Panorama de la cybermenace 2022 », 2023, [En ligne]. Disponible sur : https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/ (consulté le dec. 6, 2023).

[21] W. Zirar, « Cybersécurité : le cert santé recense 588 déclarations d'incidents en 2022 », février 2022, [En ligne]. Disponible sur : https://www.ticsante.com/story?ID=6572 (consulté le sept. 20, 2023).

[22] J.-M. Manach, « Cybersécurité : le cert santé relève 5 mises en danger patient avérées en 2021 », Next, mai 2022, [En ligne]. Disponible sur : https://next.ink/1886/cybersecurite-cert-sante-releve-5-mises-en-danger-patient-averees-en-2021/ (consulté le dec. 6, 2023).

[23] D. Mennecier, « Cyberattaques et hôpital », Médecine de Catastrophe - Urgences Collectives, vol. 4, no. 4, p. 327–330, décembre 2020.

[24] S. Smith, « Smart hospitals to deploy over 7 million internet of medical things », Juniper Research, janvier 2022, [En ligne]. Disponible sur : https://www.juniperresearch.com/press/smart-hospitals-to-deploy-over-7mn-iomt (consulté le dec. 19, 2023).

[25] Agence du Numérique en Santé, Guide « La sécurité numérique, socle de la transformation du numérique en santé », 2021, [En ligne]. Disponible sur : https://industriels.esante.gouv.fr/sites/default/files/media/document/cybersecurite_3_volets_a4_210607.pdf (consulté le dec. 3, 2023).

[26] Relyens, « Etablissement de santé : combien coûte une cyberattaque ? » octobre 2023, [En ligne]. Disponible sur : https://www.relyens.eu/fr/newsroom/blog/cybersecurite-comment-estimer-le-cout-dune-cyberattaque-par-rancongiciel (consulté le dec. 6, 2023).

[27] Agence du Numérique en Santé, « L'observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social 2022 est en ligne ! », juin 2023, [En ligne]. Disponible sur : https://esante.gouv.fr/espace-presse/lobservatoire-des-incidents-de-securite-des-systemes-dinformation-pour-les-secteurs-sante-et-medico-social-202 (consulté le dec. 19, 2023).

[28] F. Reynaud and L. Adam, « Cyberattaque contre l'hôpital de Corbeil-Essonnes : ce que l'on sait sur les données diffusées », Le Monde.fr, septembre 2022, [En ligne]. Disponible sur : https://www.lemonde.fr/pixels/article/2022/09/26/apres-la-cyberattaque-contre-l-hopital-de-corbeil-essonnes-ce-que-l-on-sait-sur-les-donnees-diffusees_6143245_4408996.html (consulté le dec. 6, 2023).

[29] « L'hôpital de Corbeil-Essonnes veut renforcer sa sécurité informatique », 20MINUTES, janvier 2023, [En ligne]. Disponible sur : https://www.20minutes.fr/societe/4017361-20230104-corbeil-essonnes-cinq-mois-apres-cyberattaque-hopital-renforce-securite-informatique (consulté le sept. 20, 2023).

[30] S. Nogaret, « Cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie », ANSM, 2022, [En ligne]. Disponible sur : https://ansm.sante.fr/documents/reference/cybersecurite-des-dm-et-dmdiv (consulté le sept. 20, 2023).

[31] V. Boissart, D. Laurent, L. Monnin, M.-J. Ory, F. Raji, and S. Roussel, « Groupe de travail afib 2019–2020 : Sécurité numérique des équipements biomédicaux », IRBM News, vol. 42, no. 1, p. 18, février 2021.

[32] Agence Régionale de Santé de la Réunion, « Cybersécurité : comment protéger les données de santé des réunionnais ? », mars 2023, [En ligne]. Disponible sur : https://www.lareunion.ars.sante.fr/cybersecurite-comment-proteger-les-donnees-de-sante-des-reunionnais (consulté le dec. 6, 2023).

[33] C. Duval, « Cyberattaques : scénarios redoutés par les hôpitaux », TGS France, mars 2021, [En ligne]. Disponible sur :

https://www.tgs-france.fr/blog/cyberattaques-scenarios-redoutes-par-les-etablissements-hospitaliers-et-medico-sociaux/(consulté le dec. 6, 2023).

[34] R. Parodi, « Informatique biomédicale exploitation des données biomédicales et organisation des fonctions supports », juin 2023, [En ligne]. Disponible sur : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids198 (consulté le sept. 20, 2023).

[35] B. Benque, « Un accompagnement institutionnel fort pour une intégration DSI », Cadresanté, octobre 2023, [En ligne]. Disponible sur : https://www.cadredesante.com/spip/profession/management/article/un-accompagnement-institutionnel-fort-pour-une-integration-dsi-biomedical-reussie (consulté le dec. 6, 2023).

[36] Commission Européenne, septembre 2023, « Directive on measures for a high common level of cybersecurity across the union (Directive NIS2) », [En ligne]. Disponible sur : https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (consulté le dec. 19, 2023).

[37] Vie-Publique, « Projet de loi visant à sécuriser et réguler l'espace numérique », octobre 2023, [En ligne]. Disponible sur : https://www.vie-publique.fr/loi/289345-projet-de-loi-numerique-sren (consulté le dec. 19, 2023).

[38] Agence nationale de la sécurité des systèmes d'information, « 5 réflexes à avoir lors de la réception d'un courriel », 2023, [En ligne]. Disponible sur : https://www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/ (consulté le nov. 3, 2023).

[39] C. Blanc-Rolin, « Sécurité, RGPD code de la santé publique : les ports USB devraient-ils rester fermés ? » février 2019, [En ligne]. Disponible sur : https://www.dsih.fr/article/3233/securite-rgpd-code-de-la-sante-publique-les-ports-usb-devraient-ils-rester-fermes.html (consulté le nov. 3, 2023).

[40] Agence nationale de la sécurité des systèmes d'information, « Attaques par rançongiciels, tous concernés. comment les anticiper et réagir en cas d'incident ? », août 2020, [En ligne]. Disponible sur : https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/(consulté le nov. 3, 2023).

[41] J. Lhomme, J. Humbert, and G. Farges, « La criticité des dispositifs médicaux : état de l'art et calcul », IRBM News, vol. 34, no. 5-6, pp. 150–154, octobre 2013.

[42] Agence du Numérique en Santé, « La cybersécurité pour le social et le médico-social en 13 questions », octobre 2022, [En ligne]. Disponible sur : https://esante.gouv.fr/actualites/un-nouveau-guide-cybersecurite-destination-du-medico-social (consulté le nov. 3, 2023).