2024-2025

HOUMADI Zaïdatte

Mémoire de fin d'études, 2ème année de Master

Management des établissements de santé, médico-sociaux, de la qualité, des risques et des flux

---

Dans quelle mesure le programme Cybersécurité accélération et Résilience des Établissements (CaRE) permet-il aux établissements de santé de gérer les crises liées aux cyberattaques et quels enseignements tirer de la méthode EBIOS RM pour renforcer cette résilience ?

Sous la direction de Christian VILHELM

Composition des membres du jury :

- Présidente du jury : Caroline LANIER, Professeure des universités ILIS
- Directeur de mémoire : Christian VILHELM, Maître de conférence à l'UFR3S, université de Lille
- Troisième membre du jury : Céline DETEZ DE LA DRÈVE, directrice des résidences seniors

Date de la soutenance : 7 juillet 2025 à 16 h

Faculté d'Ingénierie et Management de la Santé - ILIS

42 rue Ambroise Paré

59120 LOOS

Remerciements

Ce mémoire est le fruit de plusieurs mois de travail et de réflexion, et sa réalisation n'aurait pas été possible sans le soutien et l'accompagnement de nombreuses personnes. Je tiens à exprimer ma profonde gratitude à chacun d'entre eux.

En premier lieu, je souhaite adresser mes plus sincères remerciements à mon directeur de mémoire, **Monsieur Christian VILHELM**, Maître de conférences à l'UFR3S, Université de Lille. Sa disponibilité, ses conseils précieux, ses relectures attentives et ses encouragements constants ont été déterminants dans l'élaboration et la structuration de ce travail. Sa rigueur intellectuelle et sa bienveillance m'ont permis de progresser tout au long de ce projet.

Je tiens à remercier également l'ensemble des professionnels des différents établissements, qui constituent les terrains d'enquête, pour leur disponibilité, leur gentillesse et leur contribution fructueuse à ce travail de recherche qu'est le mémoire de fin d'études.

Je remercie également **Madame LANIER CAROLINE**, Professeure des universités ILIS et Présidente du jury, ainsi que **Madame DETEZ DE LA DRÈVE Céline**, pour avoir accepté d'évaluer ce mémoire et pour l'intérêt qu'ils porteront à cette recherche. Leurs remarques et questions lors de la soutenance seront une source d'enrichissement précieuse.

Mes remerciements s'adressent également à l'ensemble du corps professoral de la Faculté d'Ingénierie et Management de la Santé (ILIS), qui a su nous transmettre un savoir riche et des compétences essentielles tout au long de ces deux années de Master. Je pense particulièrement aux intervenants qui ont éclairé ma compréhension des enjeux de la cybersécurité et de la gestion des crises en santé.

Enfin, je ne saurais terminer sans remercier ma famille et mes proches pour leur soutien indéfectible. Leur patience, leur compréhension et leurs encouragements ont été une force majeure tout au long de cette période exigeante.

À toutes et à tous, merci.

Sommaire

Remerciements 2

Sommaire 3

Introduction 5

PARTIE I : CYBERSÉCURITÉ EN SANTÉ : DE LA GESTION DES RISQUES À LA GESTION DE CRISE 8

1. Définitions 8

2. Typologie et impacts des cyberattaques en santé 9

3. Enjeux spécifiques au secteur hospitalier 13

4. Cadre réglementaire et politique publique 14

PARTIE II : ANTICIPER POUR MIEUX GÉRER : LES OUTILS STRATÉGIQUES EN AMONT DE LA CRISE 18

1. Présentation de la méthode EBIOS Risk Manager 18

2. Application potentielle ou réelle dans les établissements de santé 20

3. Limites de l'approche purement anticipative face aux cyberattaques actuelles 24

PARTIE III : LE PROGRAMME CYBERSÉCURITÉ ACCÉLÉRATION, RÉSILIENCE DES ÉTABLISSEMENTS : RÉPONSES AUX CRISES CYBER EN MILIEU HOSPITALIER 28

1. Genèse, objectifs et structure du programme CaRE 28

2. Dispositifs et actions en cas de cybercrise 30

3. Forces et faiblesses de CaRE dans sa mise en œuvre concrète 32

4. Analyse comparative des forces de CaRE et des axes d'amélioration inspirés d'EBIOS 34

PARTIE IV : TERRAIN ET RETOURS D'EXPÉRIENCE 37

1. Méthodologie de l'étude qualitative 37

2. État des lieux de la gestion des cyber-risques dans les établissements de santé 42

3. Le programme CaRE à l'épreuve du terrain : Analyse de son impact sur la gestion des crises cyber 45

4. La méthode EBIOS : levier pour renforcer la résilience 48

5. Synergie et complémentarité perçues entre EBIOS et CaRE 52

PARTIE V : PRÉCONISATIONS STRATÉGIQUES POUR UNE CYBERSÉCURITÉ INTÉGRÉE..... 55

1. Des cadres nationaux à la résilience..... 55

2. Recommandations concrètes pour les établissements..... 57

3. Perspectives : vers une culture de la cybersécurité en santé..... 62

4. Limites de l'étude et pistes de recherche futures..... 63

CONCLUSION GÉNÉRALE..... 68

Bibliographie..... 69

Abréviations..... 79

Annexes..... 1

Introduction

Le 21 août 2022, le Centre Hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes est brutalement paralysé par une cyberattaque. Les systèmes informatiques tombent, les accès aux dossiers médicaux sont coupés, la coordination des soins est gravement compromise. Pendant plusieurs jours, les équipes hospitalières doivent basculer en mode dégradé, recourant au papier et au téléphone, au risque de perdre un temps précieux dans la prise en charge des patients et garantir la qualité des soins [1].

Cet incident, loin d'être isolé, illustre l'extrême fragilité numérique de notre système de santé. Il révèle une réalité encore trop sous-estimée : les établissements hospitaliers sont devenus des cibles privilégiées des cybercriminels. Leur attractivité repose sur plusieurs facteurs bien connus : infrastructures obsolètes [2], interconnexion croissante des équipements [3], manque de sensibilisation des personnels [4] et surtout, la valeur élevée des données médicales sur les marchés clandestins [5].

Mais au-delà du constat technique ou économique, ces attaques posent une question centrale : **les établissements de santé sont-ils réellement capables de faire face à une crise numérique majeure ?** Car une cyberattaque ne se limite pas à une défaillance technique, elle désorganise l'hôpital dans toutes ses dimensions : logistique, soin, communication, gouvernance et se rapproche bien davantage d'un scénario de crise systémique que d'un simple incident de sécurité.

Pendant longtemps, la cybersécurité en santé a été abordée sous l'angle de la prévention et de la conformité réglementaire : sécuriser les accès, protéger les données, répondre aux audits [6]. Pourtant, les événements récents montrent que cette approche est insuffisante. En effet, face à la sophistication et à la massification des cybermenaces, il est désormais largement reconnu que la sécurité absolue est inatteignable, faisant de l'occurrence d'un incident une certitude plutôt qu'une simple éventualité [7]. Lorsque l'attaque survient, ce n'est plus un référentiel de l'Organisation internationale de normalisation (ISO) qu'il faut mobiliser, mais une organisation prête à absorber le choc, capable de réagir rapidement, de maintenir ses activités vitales tout en protégeant les patients. Autrement dit, la cybersécurité ne relève plus uniquement de la gestion des risques, mais aussi et surtout de la gestion des crises.

Dans cette optique, deux dispositifs méritent une attention particulière :

- Le programme CaRE (Cybersécurité Accélération et Résilience des Établissements), lancé en 2022 par l'État, propose un accompagnement structuré visant à renforcer la capacité des établissements à faire face aux cyberattaques.
- La méthode EBIOS, issue du monde industriel, offre une approche stratégique pour modéliser les risques cyber en amont et orienter les décisions de sécurité.

Ces deux approches poursuivent des finalités complémentaires : EBIOS aide à anticiper les risques, CaRE structure la réponse en situation de crise. Pourtant, leur articulation reste encore marginale dans les établissements de santé et leur intégration dans les pratiques managériales est largement perfectible.

Dès lors, ce mémoire s'attache à répondre à une question centrale :

Dans quelle mesure le programme CaRE permet-il aux établissements de santé de gérer les crises cyber et en quoi la méthode EBIOS pourrait-elle enrichir cette approche pour renforcer leur résilience ?

Pour répondre à cette problématique, ce travail mobilise une double approche théorique et empirique :

- Une analyse documentaire sur les cyberattaques en santé, les enjeux de continuité d'activité et les méthodologies de gestion des risques.
- Une enquête de terrain qualitative, menée auprès de professionnels hospitaliers, afin d'évaluer la mise en œuvre réelle de ces outils, les blocages rencontrés, mais aussi les bonnes pratiques observées.

Cette approche vise à produire des recommandations concrètes et réalistes, à partir de la convergence entre théorie, méthode et expérience terrain.

Ce mémoire se structure en cinq parties progressives :

1) La première partie pose le cadre conceptuel et réglementaire de la cybersécurité hospitalière et montre, en quoi les cyberattaques doivent être abordées comme des crises systémiques.
2) La deuxième partie analyse la méthode EBIOS comme outil stratégique d'anticipation, en évaluant son applicabilité dans le secteur de la santé.
3) La troisième partie étudie le programme CaRE dans sa logique de réponse à crise, ses apports et ses limites dans la mise en œuvre.

4) La quatrième partie confronte les approches théoriques aux retours d'expérience de terrain, pour identifier les écarts et leviers d'amélioration.

5) Enfin, la cinquième partie propose des préconisations stratégiques pour renforcer la résilience cyber des établissements de santé, en articulant gestion des risques et gestion de crise.

PARTIE I : CYBERSÉCURITÉ EN SANTÉ : DE LA GESTION DES RISQUES À LA GESTION DE CRISE

1. Définitions

a) Cybersécurité, cyber risque et crise cyber

La cybersécurité constitue un domaine clé de la sécurité globale des systèmes d'information. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), elle est définie comme « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles ».

Le cyber-risque représente quant à lui la possibilité qu'une menace exploitant une ou plusieurs vulnérabilités impacte les activités opérationnelles, financières ou réputationnelles d'une organisation [8]. Il est généralement mesuré en croisant trois facteurs essentiels :

- La menace ;
- La vulnérabilité ;
- L'impact potentiel [9].

Dans les établissements de santé, ce risque revêt une importance particulière compte tenu de la sensibilité des données traitées et des répercussions potentielles sur la continuité des soins.

Ce qui induit par la même occasion, la crise cyber. Elle se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes et perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques.

C’est donc un événement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l’organisation, [10].

b) La gestion des risques et la gestion de crise.

La gestion des risques consiste en une démarche proactive visant à anticiper, identifier, analyser et traiter les risques numériques afin d’en diminuer la probabilité ou l’impact potentiel [11]. Elle inclut généralement une identification méthodique des vulnérabilités, une évaluation précise des risques et la mise en œuvre d’actions préventives adéquates [12].

En revanche, la gestion de crise intervient de façon réactive lorsqu’un incident majeur survient effectivement. Elle a pour objectif premier de limiter les conséquences immédiates d’une attaque, assurer la continuité des opérations critiques, restaurer les systèmes et services affectés et communiquer efficacement en interne et en externe pour gérer l’impact réputationnel [13].

Bien que ces deux démarches interviennent à des moments différents (avant l'incident pour la gestion des risques, après pour la gestion de crise), leur articulation s’avère essentielle dans une stratégie globale de cybersécurité efficace et adaptée à la réalité opérationnelle du secteur hospitalier.

Cette complémentarité stratégique constitue précisément l’objet central de cette recherche, qui vise à étudier comment une meilleure préparation anticipative peut renforcer significativement la capacité des établissements de santé à réagir efficacement aux cybercrises.

2. Typologie et impacts des cyberattaques en santé

Le secteur de la santé est devenu ces dernières années une cible privilégiée des cyberattaques, notamment en raison de la criticité des données traitées et de l’importance vitale des systèmes informatiques hospitaliers [14]. Ces attaques se manifestent sous diverses formes, combinant souvent un vecteur d'attaque (le moyen d'accéder au système d'information) et une charge utile (l'action malveillante exécutée et ses conséquences).

a) Les vecteurs d'attaque courants

Parmi les vecteurs d'attaque les plus fréquents, le phishing ciblé (hameçonnage) se distingue. Il représente très souvent la première étape et la plus simple pour obtenir un accès au système d'information. Ces escroqueries personnalisées visent un individu, un groupe ou une entreprise spécifique pour inciter les victimes à divulguer des données sensibles, à télécharger des logiciels malveillants ou à effectuer des transferts financiers [15]. Ce phénomène demeure une menace majeure, exploitant fréquemment le manque de sensibilisation des personnels hospitaliers.

D'autres vecteurs incluent l'exploitation de failles logicielles, les attaques via des prestataires externes ou la chaîne d'approvisionnement, ou encore l'utilisation de techniques d'ingénierie sociale au-delà du simple hameçonnage.

b) Les charges utiles et leurs conséquences

Une fois l'accès obtenu, différentes charges utiles peuvent être déployées, chacune entraînant des conséquences distinctes :

- **Les attaques par ransomware (rançongiciel)** : particulièrement destructrices dans les établissements hospitaliers. Elles consistent à chiffrer les données ou les systèmes d'information et à réclamer une rançon en échange du rétablissement des accès. L'attaque contre le Centre Hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes en août 2022 est emblématique. Elle a entraîné un blocage massif pendant plusieurs semaines, perturbant gravement l'activité médicale, l'accueil des patients et l'accès aux dossiers médicaux [1]. De telles attaques révèlent non seulement des faiblesses techniques ou organisationnelles, mais aussi des carences majeures en matière de gestion anticipée des crises.
- **Vol ou fuite massive de données de santé** : Ces attaques, souvent facilitées par le phishing ou l'exploitation de vulnérabilités, entraînent une perte de confidentialité des données médicales sensibles, leur détournement ou leur utilisation malveillante [15]. Les conséquences sont multiples : atteinte à la vie privée des patients, risques juridiques pour les établissements et dégradation de leur réputation.
- Attaque par déni de service (DDoS) : Moins fréquente dans le secteur de la santé, mais néanmoins présente, cette charge utile vise à rendre un service indisponible en submergeant le système de requêtes, perturbant ainsi l'accès aux plateformes et aux informations vitales.

- Infiltration silencieuse des systèmes informatiques : Parfois, l'objectif initial n'est pas une action immédiate mais une implantation durable au sein du système. Cela permet aux attaquants d'espionner, de voler des informations sur le long terme, ou de préparer une attaque plus grave et ciblée ultérieurement [15].

c) L'ampleur de la menace et ses coûts

D'après l'Observatoire des incidents de sécurité et système d'information, la fréquence et la sophistication des attaques contre les établissements de santé ne cessent d'augmenter [16]. En 2022, le nombre de cyberattaques majeures dans le secteur hospitalier français a augmenté de 30 % par rapport en 2021, représentant environ 10 % du total des cyberattaques en France [17].

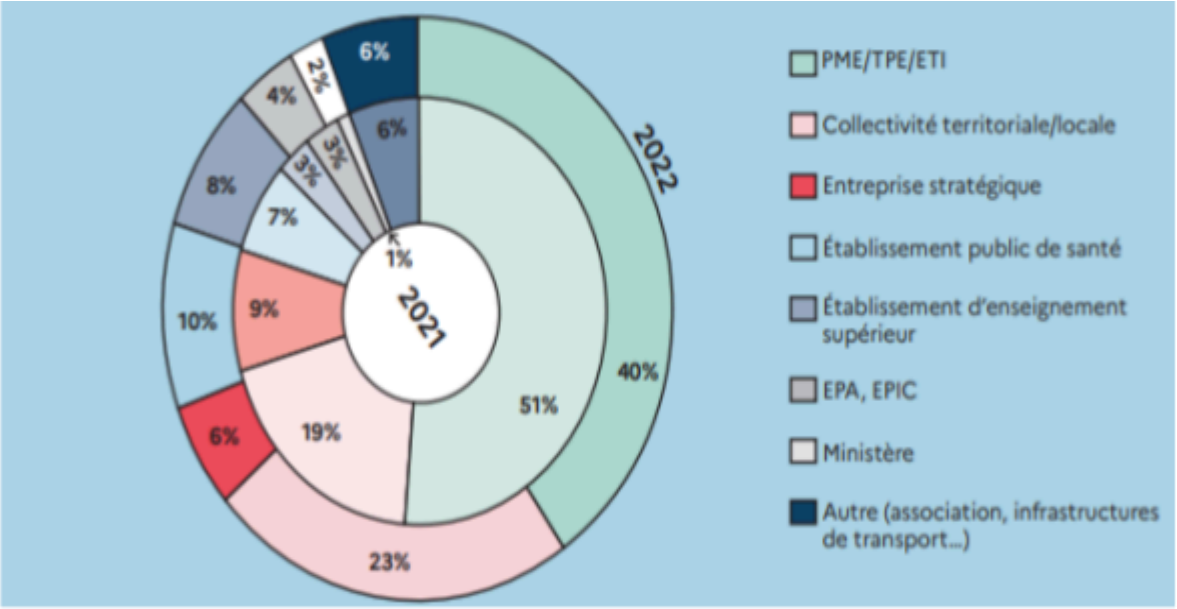

Figure 1 : répartition des types de victimes de compromissions par rançongiciel en 2021 et 2022 (ANSSI)

Au-delà de la nature technique des attaques, leurs impacts sur les établissements de santé sont considérables et multidimensionnels. Sur le plan financier, ces attaques génèrent des pertes considérables. Au-delà des coûts directs liés à la remédiation technique (rétablissement des systèmes, investigation forensique) et aux éventuelles rançons, les cyberattaques entraînent des coûts indirects souvent bien plus élevés et difficiles à quantifier.

Ces coûts indirects incluent :

- La perte de productivité due à l'interruption prolongée des activités cliniques et administratives.
- Les dépenses juridiques et les amendes réglementaires potentielles, notamment en cas de non-conformité au Règlement Général sur la Protection des Données (RGPD) ou à d'autres législations sur la protection des données.
- Le préjudice réputationnel et la perte de confiance des patients et des partenaires, peuvent entraîner des conséquences à long terme sur l'image et l'attractivité de l'établissement.
- Les coûts liés à la communication de crise et au support psychologique pour le personnel et les patients affectés.

À l'échelle mondiale, le secteur de la santé est celui où le coût moyen d'une violation de données est le plus élevé de tous les secteurs, atteignant en 2024 un montant estimé à 11,68 millions de dollars US par incident [18]. Ce chiffre, issu d'études reconnues internationalement, inclut l'ensemble des facteurs directs et indirects, soulignant l'impératif pour les établissements de santé de renforcer leur posture de cybersécurité non seulement en prévention mais aussi en capacité de résilience.

d) Une réalité critique

D'un point de vue critique, on observe que les établissements de santé se trouvent aujourd'hui souvent en posture réactive, subissant des attaques sans avoir réellement anticipé la complexité de la réponse opérationnelle nécessaire. Malgré la multiplication des alertes et recommandations institutionnelles, notamment les alertes régulières de l'ANSSI, la maturité globale des établissements reste très hétérogène, révélant un clivage profond entre les politiques publiques affichées et la réalité opérationnelle sur le terrain. Cette réalité interroge directement l'efficacité des dispositifs actuels de prévention et de réponse aux cyberattaques.

Ainsi, au-delà de la typologie technique des attaques, c'est la faiblesse structurelle des systèmes de préparation, d'alerte et de réponse qui mérite une réflexion approfondie. L'enjeu n'est pas seulement technique, mais également managérial et stratégique. Il nécessite une véritable prise en compte de la cybersécurité comme enjeu de santé publique à part entière, impliquant une approche systémique et intégrée.

3. Enjeux spécifiques au secteur hospitalier

Les établissements de santé constituent une cible particulièrement vulnérable face aux cyberattaques en raison de trois enjeux majeurs : la continuité des soins, la confidentialité des données et les considérations éthiques liées à la sécurité des patients. Ces spécificités impliquent une criticité renforcée en matière de cybersécurité et imposent aux hôpitaux des responsabilités spécifiques allant bien au-delà des seuls aspects techniques.

a) Enjeu sur la continuité des soins

Le premier enjeu essentiel concerne la continuité des soins. Une interruption des systèmes informatiques peut entraîner des conséquences immédiates et dramatiques : blocage des urgences, indisponibilité des résultats médicaux critiques ou arrêt des traitements automatisés, par exemple dans les unités de soins intensifs. L'attaque du CHU de Rouen en 2019 a illustré cette réalité avec une interruption partielle des soins pendant plusieurs jours [19]. Cet incident révèle une lacune majeure : la fragilité des processus d'urgence, souvent conçus sans tenir compte du risque numérique dans leur dimension opérationnelle.

b) Enjeu sur la confidentialité des données

Le deuxième enjeu fondamental porte sur la confidentialité des données des patients, qui sont par définition ultra-sensibles. Les données de santé constituent aujourd'hui un actif particulièrement convoité par les cybercriminels, en raison de leur haute valeur marchande sur le marché noir du numérique [20]. Contrairement à de simples numéros de carte bancaire, les données médicales peuvent être utilisées pour des fraudes plus complexes, du chantage, ou même des usurpations d'identité durables, ce qui explique leur prix élevé.

Malgré un cadre juridique contraignant avec le Règlement Général sur la Protection des Données (RGPD) et des normes spécifiques (Hébergement des données de santé : HDS), la réalité montre que de nombreux établissements ne respectent pas pleinement ces standards, exposant ainsi patients et établissements à des risques juridiques importants. Cette non-conformité expose non seulement les patients à des risques importants de divulgation de leurs informations privées, mais aussi les établissements à de lourdes sanctions financières et à des préjudices réputationnels significatifs.

c) Enjeu sur l'éthique

Enfin, l'enjeu éthique est incontournable. Il touche directement à la responsabilité morale, professionnelle des établissements et du personnel soignant face aux risques cyber. Lorsqu'une cyberattaque se produit, l'impact humain direct, tel que le report de chirurgies vitales ou la perte d'accès à des données médicales capitales pour la prise de décisions thérapeutiques, soulève des questions éthiques complexes sur la responsabilité des établissements [21]. Cette dimension éthique est encore peu intégrée dans les démarches concrètes de gestion des risques cyber, ce qui constitue une déficience préoccupante des approches actuelles.

Ces trois enjeux majeurs sont traités en silos, de façon séparée, ce qui réduit la capacité réelle des établissements à développer une résilience intégrée face aux cybermenaces. La continuité est vue comme un problème technique, la confidentialité des données comme un enjeu juridique et l'éthique comme un débat secondaire. Or, la cybersécurité hospitalière devrait les articuler dans une logique unique et cohérente, ce qui reste un défi majeur.

4. Cadre réglementaire et politique publique

Les hôpitaux évoluent dans un environnement réglementaire et normatif dense en matière de cybersécurité, ce qui conditionne fortement les politiques de sécurité numérique mises en place au sein des établissements de santé. Ce cadre est composé à la fois de réglementations européennes, nationales et de normes spécifiques visant à structurer et guider les démarches des établissements.

a) Réglementation européenne

Au niveau européen, le Règlement Général sur la Protection des Données [22] établit une base juridique contraignante pour la protection des données personnelles, particulièrement rigoureuse lorsqu'il s'agit de données de santé. Cette exigence implique pour les hôpitaux une obligation stricte de sécurisation des données des patients, sous peine de sanctions financières et réputationnelles majeures en cas de manquement ou de fuite [23]. Or, dans la pratique, la mise en conformité avec le RGPD reste inégale et souvent partielle, du fait de contraintes budgétaires, organisationnelles et humaines importantes, limitant la capacité effective des établissements à répondre pleinement aux exigences réglementaires.

b) Réglementation nationale

Au niveau national, la Loi de Programmation Militaire (LPM) [24] impose aux opérateurs de services essentiels (OSE), une catégorie incluant les établissements de santé, une obligation formelle de sécurisation de leurs systèmes d'information, ainsi que des déclarations obligatoires auprès de l'ANSSI en cas d'incidents majeurs.

c) Les normes

Sur le plan normatif, le standard international ISO 27001 [25] concernant le management de la sécurité des systèmes d'information constitue une référence importante pour guider les établissements dans leurs démarches internes de sécurisation [26]. De même, le référentiel Hébergeur de Données de Santé (HDS) [27] établit des exigences techniques et organisationnelles spécifiques aux prestataires et hôpitaux qui stockent ou traitent des données médicales sensibles [28]. Toutefois, ces normes et certifications, bien que pertinentes, peuvent être perçues par les établissements comme trop complexes, coûteuses et éloignées de leurs réalités opérationnelles, qui peuvent limiter leur adoption généralisée.

Face à ces défis, le ministère de la santé et des solidarités a lancé en 2021 le programme national Cybersécurité accélération et Résilience des Établissements (CaRE), destiné à améliorer la réponse opérationnelle et stratégique des établissements face aux cyberattaques [29]. Cette initiative traduit la reconnaissance politique explicite d'une insuffisance structurelle antérieure. Il ambitionne d'accompagner les hôpitaux dans la mise en sécurisation de leurs systèmes et la mise en place de plan de continuité. Toutefois, si les ambitions affichées par CaRE sont claires, sa mise en œuvre opérationnelle demeure améliorable, notamment en raison d'une diversité importante des niveaux de maturité et de ressources des établissements concernés.

De manière critique, il apparaît que ce cadre réglementaire et normatif ambitieux ne parvient pas pleinement à produire les effets escomptés. L'écart important entre les obligations théoriques et les pratiques concrètes des établissements révèle une difficulté majeure : celle d'articuler efficacement le normatif, le juridique, le technique et l'opérationnel dans des établissements soumis à des contraintes organisationnelles fortes.

Figure 2 : Organigramme de la direction d'un CHU, avec identification des services clés pour la gouvernance et l'opérationnalisation de la cybersécurité.

Cette Figure 2 illustre l'organigramme de la direction d'un CHU. Les directions encerclées représentent les services clés dont la collaboration est essentielle à une cybersécurité intégrée. la Direction générale et la Direction générale adjointe (pour la vision stratégique globale), la Direction de crise (pour la gestion opérationnelle des incidents), la Direction des risques cyber et la Direction qualité, sécurité et pertinence des soins (pour la gouvernance des risques et la conformité), la Direction du numérique (pour l'implémentation technique et la gestion des SI) et la Direction des affaires juridiques et éthiques, transparence et probité (pour les aspects légaux et la protection des données), ainsi que la Coordination générale des soins et recherche paramédicale (représentant les enjeux opérationnels et les utilisateurs finaux).

Bien que cette répartition des fonctions soit nécessaire pour la spécialisation des tâches, elle peut, en pratique, conduire à un fonctionnement en silos. Les services opèrent souvent avec des priorités, des langages et des canaux de communication propres. Cette segmentation rend complexe l'articulation fluide et la coordination transversale des

exigences de cybersécurité, qui par nature, nécessitent une compréhension holistique des enjeux normatifs, juridiques, techniques et opérationnels à l'échelle de l'établissement. Une coordination efficace entre ces entités est donc un facteur critique pour transformer les cadres réglementaires en une posture de cyber-résilience concrète.

Ainsi, au-delà d'un simple renforcement réglementaire, la cybersécurité hospitalière nécessite un accompagnement pragmatique et adapté, tenant compte des réalités spécifiques du secteur, pour permettre une véritable intégration de la sécurité numérique dans la culture organisationnelle des établissements de santé.

La multiplication des cyberattaques dans le secteur hospitalier met en lumière une tension fondamentale entre urgence opérationnelle et anticipation stratégique. Si la gestion de crise constitue une réponse indispensable face à l'imprévisibilité de ces menaces, elle ne peut se substituer à une véritable culture de la prévention. Dans cette logique, la gestion des risques apparaît comme un levier incontournable pour renforcer la résilience organisationnelle.

La partie suivante s'attache ainsi à explorer les outils et méthodes mobilisables en amont de la crise, en mettant l'accent sur la méthode EBIOS, largement utilisée dans l'industrie et dont les principes pourraient enrichir la stratégie de cybersécurité des établissements de santé. Cette analyse permettra de mieux cerner les apports réels de l'approche anticipative, mais aussi ses limites face aux dynamiques d'attaque de plus en plus rapides, complexes et ciblées.

PARTIE II : ANTICIPER POUR MIEUX GÉRER : LES OUTILS STRATÉGIQUES EN AMONT DE LA CRISE

1.Présentation de la méthode EBIOS Risk Manager

Dans le paysage français de la cybersécurité, la méthode Expression des Besoins et Identification des Objectifs de Sécurité, Risk Manager (EBIOS RM) s'est affirmée comme une référence incontournable en matière d'analyse et de gestion des risques numériques. Élaborée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) [30], elle est aujourd'hui largement utilisée dans des secteurs sensibles tels que la défense, l'énergie, les finances et tend progressivement à s'implanter dans d'autres secteurs critiques, dont la santé.

À son origine, la méthode EBIOS RM a été conçue pour répondre à un besoin précis : fournir aux organisations une démarche structurée mais adaptable, permettant d'intégrer efficacement les enjeux cybersécurité dans leurs stratégies globales. Depuis sa révision majeure en 2018, EBIOS RM met particulièrement l'accent sur une approche dite « orientée métiers », qui consiste à traduire les risques techniques en impacts opérationnels et stratégiques concrets pour les décideurs. Cette dimension stratégique, souvent négligée dans les démarches purement techniques, est centrale dans l'intérêt que les organisations manifestent pour cette méthode [30].

La diffusion et l'adoption de cette méthode en France sont notables : selon l'expert interrogé lors de cette recherche documentaire [31], EBIOS RM est désormais intégrée dans quasiment toutes les analyses de risques effectuées au sein des administrations publiques françaises. Elle constitue également la référence principale de la norme internationale ISO/IEC 27005, qui a été actualisée en 2022 pour être pleinement alignée avec la méthodologie française. Cette reconnaissance normative souligne non seulement l'efficacité éprouvée d'EBIOS RM mais aussi sa pertinence internationale.

La méthodologie d'EBIOS RM se structure autour de cinq ateliers successifs mais modulaires, permettant de s'adapter à la diversité des contextes organisationnels :

1. Cadrage du périmètre à protéger : identification des systèmes critiques et définition claire des limites de l'analyse.
2. Étude des événements redoutés : formalisation des impacts métier précis liés à chaque risque identifié.

3. Analyse des scénarios de menace : modélisation des attaques plausibles en fonction du profil des attaquants et des vulnérabilités potentielles.
4. Étude des mesures de sécurité existantes et projetées : évaluation de l'efficacité des protections en place et définition des mesures complémentaires nécessaires.
5. Plan d'action : hiérarchisation et planification concrète des mesures de sécurisation à court, moyen et long terme.

Cette modularité est particulièrement utile pour les établissements hospitaliers, souvent caractérisés par des contraintes humaines et financières fortes. Selon l'expert cyber d'ALL4TEC qui conçoit et distribue des outils d'analyse des risques, « *une des grandes forces d'EBIOS RM est justement son adaptabilité à la réalité opérationnelle : elle permet de conduire des analyses de risques très ciblées, comme des 'analyses flash', particulièrement efficaces dans des environnements complexes et sous tension, comme les hôpitaux* ». Concrètement, ces analyses rapides peuvent se réaliser en un ou deux jours sur un périmètre précis (par exemple, les systèmes d'information liés aux urgences ou à l'imagerie médicale), facilitant ainsi une prise en main rapide et des résultats immédiatement opérationnels.

Toutefois, en dépit de ses qualités, la pénétration réelle d'EBIOS RM dans le milieu hospitalier demeure inégale. Plusieurs obstacles opérationnels persistent :

- Une faible connaissance de la méthodologie au niveau stratégique (directions générales, médicales), ce qui réduit son impact sur la gouvernance.
- Une perception technique encore tenace, cantonnant souvent l'outil au domaine des RSSI, en contradiction avec l'ambition initiale d'une approche métier.
- Une difficulté à traduire les risques cyber en impacts concrets et compréhensibles par les non-informaticiens.

Cette dernière limite est particulièrement critique, car elle empêche une véritable appropriation stratégique de la démarche par les décideurs hospitaliers. Or, comme le souligne l'expert interrogé, « *sans une traduction claire et compréhensible des risques, les décideurs ne peuvent pas arbitrer efficacement sur les priorités réelles* ». Cela représente un enjeu majeur, car les choix stratégiques faits en amont influencent directement la capacité de réaction et la résilience face aux crises.

Enfin, il convient de rappeler une évidence parfois négligée : aucune méthode, aussi robuste soit-elle, ne peut garantir une protection absolue. Selon CERT Santé l'efficacité d'EBIOS RM dépend largement de son actualisation régulière pour prendre en compte la nature évolutive et complexe des cybermenaces actuelles. Cette dimension dynamique impose une vigilance constante, difficile à maintenir dans des établissements hospitaliers déjà surchargés.

EBIOS RM constitue un levier stratégique prometteur pour le secteur de la santé, à condition de dépasser certains obstacles culturels et organisationnels. Son succès dépendra notamment de sa capacité à être intégrée dans des démarches plus larges telles que le programme national CaRE, afin de créer une dynamique de résilience complète et durable. L'enjeu central sera ainsi de transformer cette méthode encore sous-utilisée en une pratique courante et intuitive au sein des établissements hospitaliers.

2. Application potentielle ou réelle dans les établissements de santé

Si la méthode EBIOS RM est devenue incontournable dans les secteurs régaliens et industriels français, son adoption dans le milieu hospitalier demeure à ce jour fragmentée, inégale, et souvent embryonnaire. Pourtant, comme le souligne l'expert interrogé, « *tous les centres hospitaliers français réalisent aujourd'hui une forme d'analyse des risques cyber, mais avec une grande disparité dans les méthodes employées et la qualité des résultats* ». Cette observation révèle une réalité complexe : la reconnaissance du besoin existe, mais la mise en pratique structurée et systématique fait souvent défaut.

Plusieurs facteurs structurels expliquent cette adoption encore limitée dans les établissements de santé. Premièrement, le secteur hospitalier français est caractérisé par une diversité organisationnelle unique : multiplicité des systèmes d'information (dossier patient, imagerie médicale, pharmacie), variété des métiers impliqués (médecins, personnels infirmiers, administratifs, techniques), et tensions constantes sur les ressources humaines et budgétaires. Dans un tel contexte, l'application rigoureuse d'EBIOS RM, méthode exigeante en ressources humaines et techniques, peut apparaître difficilement atteignable pour beaucoup d'hôpitaux, en particulier ceux de taille moyenne ou situés dans des territoires éloignés des grandes métropoles.

Toutefois, l'intérêt stratégique d'adopter EBIOS RM reste réel. En effet, l'approche méthodologique modulaire d'EBIOS permet des démarches ciblées et progressives, adaptées aux contraintes spécifiques du secteur hospitalier. Ainsi, l'expert interrogé insiste particulièrement sur la pertinence des « *analyses flash* », des évaluations rapides centrées sur un périmètre très précis comme les urgences, les laboratoires de biologie ou les services critiques de radiologie et d'imagerie médicale. Selon lui, « *en un ou deux jours, une équipe hospitalière peut identifier clairement ses actifs numériques essentiels, les scénarios de menace les plus plausibles, et définir des mesures correctives immédiatement opérationnelles* ». Ce format allégé facilite la sensibilisation interne et rend la démarche accessible même à des établissements disposant de peu de moyens techniques ou financiers.

a) Illustrations pratiques de la complémentarité EBIOS RM et CaRE : Retours d'expérience des professionnels de santé

Des établissements pionniers illustrent déjà le potentiel concret d'EBIOS RM en santé, ne serait-ce que par l'application des principes de gestion des risques qui sous-tendent la méthode, même sans une formalisation complète. Le programme national CaRE lui-même reconnaît explicitement la valeur stratégique de l'analyse des risques en amont, notamment pour les établissements de taille intermédiaire ou de petite taille, qui représentent la majorité du paysage hospitalier français. Ainsi, loin d'être exclue de CaRE, l'analyse des risques à travers EBIOS RM pourrait constituer un socle méthodologique essentiel permettant aux établissements de dépasser une approche purement réactive pour évoluer vers une véritable gouvernance anticipée du risque cyber.

Pour donner un caractère concret à l'articulation entre l'analyse des risques telle que formalisée par EBIOS RM et la mise en œuvre de mesures de résilience (via le programme CaRE), il est essentiel d'illustrer ces concepts par un exemple tiré de l'expérience terrain des professionnels.

Un exemple frappant de cette dynamique a été rapporté par une technicienne informatique au sein d'un établissement de santé [32]. Elle a décrit un "*incident sérieux*" survenu il y a trois ans : « *un phishing bien ficelé qui avait failli passer, mais heureusement on a réagi à temps. Depuis, on est beaucoup plus vigilants, et surtout on a compris que la gestion de crise ne se limite pas à la technique.* » Cet événement, bien que non issu d'un audit EBIOS RM formel, a agi comme un véritable "révélateur de vulnérabilités". Il a mis en

lumière un scénario de menace critique, l'ingénierie sociale via le phishing et a démontré une faiblesse dans la “dernière *ligne de défense*" : la sensibilisation du personnel. Dans le cadre d'une analyse de risques structurée avec EBIOS RM, un tel scénario aurait été identifié, évalué en termes d'impact et de vraisemblance, et aurait conduit à des recommandations spécifiques pour renforcer la posture de sécurité.

À la suite de cette expérience, l'établissement a initié la mise en place de mesures concrètes qui s'inscrivent parfaitement dans les objectifs du programme CaRE. La technicienne SI a notamment précisé : « *On essaie aussi de sensibiliser le personnel avec des petites fiches pratiques et des formations, parce que c'est l'humain la première barrière.* » Ces actions de prévention et de sensibilisation sont fondamentales pour la sécurité des systèmes d'information, et s'intègrent dans une démarche globale de renforcement de la cyber-résilience. Elles peuvent être considérées comme des actions complémentaires aux audits ciblés. Par exemple, si un audit du Domaine 1 de CaRE (audits d'annuaire et d'exposition internet) avait révélé des failles dans la gestion des comptes utilisateurs ou une surface d'attaque exposée, la sensibilisation du personnel à des menaces comme le phishing deviendrait une mesure corrective essentielle pour limiter les risques induits par ces failles techniques.

L'importance de cette approche est corroborée par le coordinateur SSE d'un autre établissement de santé, qui affirme que « *la clé, c'est l'humain. On peut avoir les meilleurs outils, les meilleurs plans, mais si les équipes ne sont pas formées, sensibilisées, et si elles ne communiquent pas efficacement en cas de crise, tout cela ne sert à rien. C'est un travail continu, une culture à instaurer. Et il ne faut pas avoir peur de faire des exercices, encore et encore, pour être vraiment prêt*. » La réalisation de ces exercices de gestion de crise, auxquels la technicienne SI participe activement dans le cadre de la mise en place de CaRE, est une composante clé d'une stratégie de continuité et de reprise d'activité. Les exercices sont une application concrète de la Stratégie de continuité et de reprise d'activité (Domaine 2 de CaRE), permettant de tester et de valider les plans mis en place suite aux audits et aux mesures préventives.

Cet exemple démontre que même sans un processus EBIOS RM pleinement implémenté, les établissements de santé sont confrontés à des problèmes qui nécessitent une détection et une réponse structurée. L'incident de phishing a servi de catalyseur pour une prise de conscience et la mise en place de mesures (sensibilisation, formations, exercices), alignées sur les préconisations du programme CaRE en matière de résilience

globale et de gestion des risques issus des audits (Domaine 1) et de la continuité/reprise d'activité (Domaine 2), confirmant ainsi la complémentarité des démarches d'analyse de risques et de résilience opérationnelle sur le terrain.

Cependant, les freins à une adoption large et systématique restent nombreux. L'une des difficultés majeures réside dans l'absence actuelle d'outils simples et adaptés spécifiquement au secteur santé. Comme l'exprime clairement l'expert interrogé, « *beaucoup d'établissements ne savent pas par où commencer, manquent de ressources internes formées à la méthodologie, et ne trouvent pas facilement de guide opérationnel adapté à leur réalité hospitalière* ». Ce manque d'accompagnement méthodologique concret constitue un obstacle majeur à la diffusion effective d'EBIOS RM dans les établissements de santé, en particulier ceux ayant le moins de moyens.

De plus, le choix du périmètre d'analyse représente un enjeu déterminant : il doit être clairement aligné sur les processus critiques qui affectent directement les soins et la sécurité des patients. En ciblant précisément les actifs numériques les plus sensibles (par exemple, les systèmes de gestion des urgences, les dossiers patients informatisés, ou encore les systèmes de télé-imagerie), l'analyse des risques prend tout son sens, non seulement pour les équipes techniques mais aussi pour les professionnels médicaux et les décideurs stratégiques. Cette démarche concrète et métier-centrée facilite aussi la communication entre les différentes parties prenantes, historiquement cloisonnées, favorisant ainsi une meilleure prise de décision collective.

Enfin, un domaine trop souvent ignoré, pourtant important, concerne la cybersécurité des activités de recherche et développement (R&D) dans les établissements hospitaliers. L'expert interrogé met en garde contre les conséquences potentiellement graves d'une fuite de données sensibles issues de la recherche clinique ou biomédicale : « *les hôpitaux sous-estiment encore fortement les risques associés à la R&D, alors même qu'une fuite d'information peut avoir des conséquences financières majeures ou même sanitaires, par exemple la fuite de données relatives à un vaccin en cours d'essai* ». Cette problématique montre une lacune persistante dans la prise en compte globale des risques numériques dans les stratégies hospitalières, soulignant le besoin urgent d'étendre le périmètre des analyses EBIOS RM à ces activités particulièrement vulnérables.

b) Des opportunités mais des freins culturels à dépasser

En synthèse, EBIOS RM dispose d'un potentiel réel pour devenir une référence méthodologique structurante dans les établissements de santé français, à condition toutefois qu'elle soit adaptée, simplifiée et largement diffusée. La méthodologie existe, elle est éprouvée dans d'autres secteurs critiques, mais le milieu hospitalier français doit encore franchir plusieurs étapes nécessaires :

- Renforcer la formation et l'acculturation à la gestion des risques cyber, au-delà des équipes techniques, auprès des équipes soignantes et des directions stratégiques ;
- Proposer des formats méthodologiques adaptés (notamment des analyses « flash » rapides et ciblées) permettant une mise en pratique accessible aux établissements les moins équipés ;
- Accompagner concrètement les établissements, via des guides pratiques et opérationnels spécifiquement dédiés à la santé, pour favoriser une appropriation réelle et durable de la méthode.

L'enjeu est bien de transformer EBIOS RM, aujourd'hui encore sous-utilisée, en un réflexe stratégique et organisationnel ancré au cœur des établissements de santé, leur permettant ainsi de gagner en maturité cyber et en résilience face aux crises futures.

3. Limites de l'approche purement anticipative face aux cyberattaques actuelles

Bien que l'approche anticipative incarnée par la méthode EBIOS Risk Manager soit essentielle pour structurer la cybersécurité hospitalière, elle présente néanmoins des limites intrinsèques face à la nature particulièrement évolutive, complexe et souvent imprévisible des cyberattaques actuelles. Comme l'exprime clairement l'expert interrogé, « *anticiper est indispensable, mais anticiper seul ne suffit pas. Mal anticiper peut même créer un faux sentiment de sécurité* ». Plusieurs facteurs expliquent pourquoi une gestion exclusivement anticipative des risques ne peut garantir une protection totale face aux crises cyber actuelles.

3.1. Une réalité cyber mouvante et incertaine

Les établissements hospitaliers évoluent aujourd'hui dans un environnement numérique complexe et instable, caractérisé par une diversification croissante des points d'entrée

possibles pour les cyberattaques. La généralisation des objets connectés médicaux, la démocratisation rapide de la télémédecine ou encore l'augmentation massive du télétravail administratif créent autant de nouvelles vulnérabilités difficiles à anticiper intégralement. À ces facteurs techniques s'ajoute la mobilité accrue des personnels hospitaliers, souvent insuffisamment formés aux bonnes pratiques de sécurité informatique, renforçant ainsi les risques de compromission.

De plus, l'écosystème des cyberattaquants se révèle particulièrement hétérogène : cybercriminels opportunistes, groupes organisés sophistiqués voire acteurs étatiques ciblant spécifiquement certaines activités hospitalières sensibles, notamment dans le domaine de la recherche biomédicale. Comme le souligne l'expert interrogé, « *beaucoup d'établissements hospitaliers ne connaissent pas réellement leurs attaquants potentiels, ni pourquoi ils seraient précisément ciblés. Cette méconnaissance conduit souvent à des scénarios d'analyse théoriques, éloignés des véritables menaces opérationnelles* ».

3.2. Des attaques innovantes et difficilement modélisables

Une seconde limite majeure tient au caractère innovant et souvent imprévisible des attaques cyber actuelles. Les cyberattaquants adoptent des stratégies hybrides sophistiquées, combinant attaques techniques complexes (ex. ransomware évolutifs) et techniques de manipulation humaine (phishing très ciblé). L'expert interrogé insiste particulièrement sur ce point : « *Les établissements se préparent souvent à des scénarios standards, mais la réalité opérationnelle montre que les cyberattaques réelles combinent souvent des techniques multiples, difficiles à prévoir précisément* ». Cette capacité d'innovation permanente des attaquants rend les analyses anticipatives des risques nécessairement incomplètes et fragiles.

Par ailleurs, il est également courant que les établissements adoptent des mesures génériques issues de référentiels standards, sans vérifier leur adéquation concrète à la réalité hospitalière. Or, comme le rappelle l'expert, « p*rès de 30 % des mesures prescrites par certains référentiels peuvent ne pas être pertinentes dans le contexte spécifique des établissements de santé, générant des dépenses inutiles et un sentiment erroné de sécurité renforcée* ».

3.3. Une gestion des risques encore trop statique et cloisonnée

Une autre limite observée est la déconnexion fréquente entre l'analyse anticipative des risques et la gestion opérationnelle effective des crises. De nombreux établissements mènent l'analyse des risques comme un exercice administratif ponctuel, souvent motivé par une obligation réglementaire ou de certification, mais ne la réactualisent pas régulièrement après des incidents ou des retours d'expérience internes. Or, comme le souligne le rapport du CERT Santé [17], une gestion efficace des risques cyber suppose précisément une boucle itérative entre anticipation et retour d'expérience terrain. En l'absence de cette dynamique, les analyses deviennent rapidement obsolètes et déconnectées des réalités opérationnelles.

3.5. Le besoin d'un écosystème intégré : anticiper et réagir

Ces limites soulignent clairement la nécessité d'inscrire l'approche anticipative dans un cadre plus large, qui intègre également des dispositifs concrets de réaction rapide et de gestion opérationnelle des crises. C'est précisément l'ambition affichée par le programme national CaRE, qui complète l'analyse anticipative des risques (EBIOS RM) par une réponse opérationnelle structurée en cas d'incident majeur, incluant des plans de continuité d'activité, une coordination renforcée et des dispositifs réguliers d'entraînement des équipes hospitalières [29].

L'expert interrogé le résume ainsi : « *EBIOS RM et CaRE ne sont pas deux démarches concurrentes, elles s'emboîtent parfaitement : l'une permet d'anticiper, l'autre de réagir efficacement lorsque l'incident survient* ». Cette complémentarité est essentielle pour garantir une résilience organisationnelle réelle, capable à la fois de prévoir et d'encaisser les crises cyber actuelles.

a) Anticiper, oui, mais sans illusion d'exhaustivité

La principale faiblesse d'une approche strictement anticipative réside dans son aspiration implicite à prévoir exhaustivement toutes les menaces possibles. Or, dans un univers cyber en constante mutation, cette exhaustivité est impossible à atteindre. La véritable résilience hospitalière ne viendra pas seulement d'une analyse des risques précise, mais de la capacité des établissements à s'adapter rapidement à l'inattendu, à tirer systématiquement parti des expériences passées, et à actualiser constamment leurs scénarios d'attaque et leurs dispositifs de réponse. Sortir d'une logique linéaire et

purement anticipative pour adopter une logique agile, itérative et transversale est désormais indispensable pour faire face aux cyberattaques actuelles.

Si la gestion anticipative des risques constitue une pierre angulaire de la résilience numérique en santé, elle ne peut à elle seule répondre à l'urgence, à la complexité et à la brutalité d'une crise cyber. Préparer, oui mais encore faut-il savoir réagir. C'est précisément pour combler cette lacune opérationnelle que le programme national CaRE (Cybersécurité accélération et Résilience des Établissements) a vu le jour. Dans cette nouvelle partie, il s'agit d'examiner comment ce dispositif institutionnel structure la réponse des établissements de santé face aux attaques, quelles en sont les limites, et surtout, en quoi il peut ou non s'articuler efficacement avec des méthodes d'anticipation comme EBIOS RM.

PARTIE III : LE PROGRAMME CYBERSÉCURITÉ ACCÉLÉRATION, RÉSILIENCE DES ÉTABLISSEMENTS : RÉPONSES AUX CRISES CYBER EN MILIEU HOSPITALIER

1. Genèse, objectifs et structure du programme CaRE

Face à la montée inquiétante des cyberattaques dans le secteur de la santé, l'État français a lancé en 2021 le programme Cybersécurité Accélération et Résilience des Établissements (CaRE) [33]. Porté par le ministère de la Santé et soutenu par l'ANSSI dans le cadre de la stratégie nationale de cybersécurité en santé. Le ministère de la Santé a intégré la cybersécurité comme axe structurant de sa feuille de route numérique 2023-2027 intitulée « Accélérer le virage numérique en santé » (action 19) [34]. Le programme CaRE s'inscrit dans le plan d'investissement global « Ségur du numérique », visant à renforcer l'infrastructure numérique des établissements de santé, tout en leur fournissant les moyens de se défendre efficacement contre les menaces cyber.

Ce programme se veut résolument opérationnel et pragmatique. Contrairement à des approches théoriques d'analyse des risques, CaRE se positionne du côté de la réaction, de la réponse et de la continuité d'activité, en partant du principe que les attaques ne sont plus une éventualité, mais une certitude.

1.1. Une réponse à un déficit structurel de préparation

Les cyberattaques majeures survenues entre 2019 et 2022, telles que celles du CHU de Rouen en 2019, du Centre Hospitalier Sud Francilien de Corbeil-Essonnes en 2022, ou encore de Dax en 2021 [35], ont mis en lumière une réalité brutale, la vulnérabilité du système de santé face à la criminalité numérique. Le manque de formation du personnel aux bonnes pratiques et la priorité donnée aux soins plutôt qu'à la protection des systèmes informatiques renforcent cette vulnérabilité [36].

Ces constats ont conduit à une prise de conscience politique : il ne suffit pas d'anticiper les risques, il faut organiser la réaction. C'est dans ce cadre que CaRE est né, avec une ambition claire : réduire les temps de blocage, limiter les pertes d'exploitation et restaurer rapidement les capacités critiques de soins en cas d'attaque.

Comme l'indique Houtain, une bonne gestion de crise repose sur la combinaison de mesures techniques et organisationnelles. Le facteur humain joue un rôle crucial, sans formation adaptée, même les meilleurs dispositifs techniques peuvent être inefficaces.

1.2. Objectifs stratégiques du programme CaRE

CaRE repose sur trois objectifs centraux :

1. Sécurisation des systèmes d'information critiques, pour éviter l'interruption des soins ou la fuite de données médicales sensibles.
2. Préparation des établissements à la gestion de crise, en intégrant la cybersécurité dans la continuité des soins et les plans d'urgence.
3. Pérennisation de l'offre de soins, y compris en cas d'attaque, via des dispositifs de reprise d'activité robustes.

Ces objectifs sont opérationnelles autour de quatre axes d'action complémentaires :

- **Gouvernance et résilience** : désignation d'un référent cyber, élaboration de plans de réponse et structurer des circuits de remontée d'information en cas d'incident ;
- **Ressources et mutualisation** : partage de bonnes pratiques, interopérabilité entre établissements au sein des GHT ;
- **Sensibilisation** : formation des professionnels aux réflexes cyber et à la culture du risque numérique ;
- **Sécurité opérationnelle** : diagnostic technique, traitement des vulnérabilités, renforcement des infrastructures critiques [37].

1.3. Structuration et financement du programme

Le programme CaRE bénéficie d'un financement public significatif, porté par la stratégie d'accélération "Santé numérique" du plan France 2030 [38].

Une enveloppe initiale de 250 millions d'euros a été mobilisée jusqu'en 2025. L'ambition affichée est d'atteindre 750 millions d'euros d'investissement d'ici 2027, pour couvrir la montée en maturité de l'ensemble des structures hospitalières et médico-sociales.

Sur le plan opérationnel, le déploiement de CaRE suit un calendrier progressif :

- 2023 : phase de pilotage dans des établissements volontaires, avec expérimentation du kit PCRA (Plan de Continuité et de Reprise d'Activité) et appui des ARS.

- 2024–2027 : généralisation à l'ensemble des établissements publics de santé, avec une montée en puissance progressive du dispositif.

a) Une réponse bienvenue, mais tardive et perfectible

L'instauration du programme CaRE représente une avancée avérée dans la prise en compte institutionnelle de la menace cyber en santé. Il permet enfin de structurer une réponse nationale cohérente, là où les établissements étaient jusqu'alors livrés à eux-mêmes. Le programme met l'accent sur la continuité des soins, ce qui est fondamental dans un contexte où chaque minute d'interruption peut entraîner des conséquences vitales.

Cependant, il faut également souligner que CaRE reste une réponse partielle. Il se concentre majoritairement sur la phase de réaction à la crise et la résilience post-attaque, sans toujours intégrer suffisamment la logique d'anticipation stratégique, notamment en matière d'analyse des risques cyber.

2. Dispositifs et actions en cas de cybercrise

Le programme CaRE se distingue par son ambition d'articuler la cybersécurité avec la continuité des soins. Là où d'autres dispositifs abordent la cybersécurité sous un prisme exclusivement technique ou normatif, CaRE propose un outillage opérationnel ciblé sur les situations de crise, en reconnaissant l'impact direct des cyberattaques sur l'offre de soins. Cette approche répond à une réalité, en cas d'attaque, ce ne sont pas les équipements qui sont en jeu, mais la capacité d'un hôpital à continuer à soigner, à opérer, à prendre en charge des urgences.

Le programme s'articule autour de deux domaines principaux d'intervention, pensés comme complémentaires, l'un concerne la prévention technique et l'autre la capacité organisationnelle à réagir.

2.1. Domaine 1 : audits techniques et remédiation des vulnérabilités

Dans ce domaine, le programme prévoit la réalisation d'audits de sécurité des systèmes d'information, ciblant notamment les éléments critiques les plus exposés :

- Les serveurs active directory, souvent mal segmentés ou obsolètes, représentent un point d'entrée majeur pour les attaquants ;
- Les expositions sur internet non maîtrisées (protocoles ouverts, équipements mal configurés) sont également systématiquement auditées.

Ces audits sont confiés à des prestataires labellisés, sélectionnés dans le cadre du marché public piloté par l'agence du numérique en santé (ANS). Ils donnent lieu à des rapports de vulnérabilités priorisés avec un plan de remédiation à échéance courte.

Le domaine exige l'atteinte d'un niveau minimal de sécurisation de ceux-ci en atteignant un score d'au moins 2 sur une échelle à 5 niveaux, sur plusieurs audits des annuaires techniques et d'avoir réalisé des audits d'exposition réguliers [39].

2.2. Domaine 2 : continuité et reprise d'activité (CRA)

Le cœur stratégique de CaRE réside dans sa volonté de formaliser des plans de continuité et de reprise d'activité (PCRA) spécifiques aux cyberattaques, une première dans le secteur hospitalier.

À la différence des audits, la composante "continuité et reprise d'activité" est toujours en attente de déploiement. Elle devrait être lancée au deuxième trimestre 2025 et achevée en juin 2026. En prélude, 28 établissements pilotes ont déjà effectué des essais [40], et la boîte à outils PCRA est opérationnelle depuis 2024.

Le PCRA intègrent plusieurs outils clés :

- La réalisation d'un bilan d'impact sur l'activité (BIA), afin d'identifier les systèmes critiques d'activités (SCA) et ceux nécessaires à la reprise d'activité (SRA) ;
- La définition de scénarios d'indisponibilité réalistes : pertes du SI global, indisponibilité d'un logiciel métier, panne réseau, etc. ;
- La mise en œuvre d'une « crash box », c'est-à-dire un plan d'action d'urgence mobilisable immédiatement (procédures papier, redondances manuelles, listage des contacts critiques, etc.)

L'ANS fournit un kit PCRA composé d'un guide méthodologique, d'un modèle de conduite de projet, de fiches sur le rôle du référent en plan de continuité et de reprise d'activité (RPCRA), ainsi que des supports pour les ateliers de sensibilisation.

Ce volet est particulièrement innovant, car il incite les établissements à intégrer le risque cyber dans les plans de crise existants (plan blanc, Vigipirate, etc.), encore trop souvent

déconnectés du numérique. Le binôme RPCRA-RSSI devient alors un levier de coordination entre la gouvernance informatique et la gouvernance médicale.

2.3. Soutiens externes, partenariats et mutualisation

Pour accompagner la montée en compétence des établissements, le programme CaRE propose :

- Un soutien actif des Agences Régionales de Santé (ARS), qui assurent l'accompagnement méthodologique, le suivi des financements et l'animation territoriale ;
- Le recours possible à des prestataires extérieurs pour les missions techniques (diagnostic, mise en conformité, formation) ;
- La mutualisation d'expérience au sein des groupements hospitaliers de territoires (GHT), pour favoriser la montée en compétences collectives et éviter les doublons.

La mutualisation reste un enjeu fort. Dans un secteur où les ressources sont inégalement réparties, la capacité à partager les retours d'expériences et à harmoniser les pratiques est essentielle pour éviter la fracture numérique entre grands CHU et petits hôpitaux de proximité.

2.4. Un pas décisif, mais pas encore structurant

CaRE a le mérite de rendre enfin concrète et actionnable la question de la cybercrise en santé. Il ne s'agit plus d'un sujet technique réservé à l'informatique, mais bien d'un sujet de gouvernance hospitalière, avec une méthode, des outils, des financements, et une doctrine claire.

Cependant, la moitié de la réponse (continuité d'activité) étant encore en cours de développement, la résilience cyber reste inachevée : le programme pose de bonnes bases, mais laisse les établissements seuls face à la dernière ligne droite, celle qui consiste à traduire les principes en pratiques concrètes.

3. Forces et faiblesses de CaRE dans sa mise en œuvre concrète

Le programme représente indéniablement une étape majeure dans la gestion des cybercrises hospitalières. Il a permis de sortir la cybersécurité du domaine informatique

pour en faire un enjeu collectif et organisationnel. Cependant, la concrétisation de ses outils et principes met en lumière une réalité plus complexe. Si des avancées sont palpables, le programme se heurte encore à des freins culturels, structurels et humains qui persistent.

3.1. Les forces, premiers acquis et dynamiques positives

a) Une prise de conscience à tous les niveaux

Avant le programme CaRE, la cybersécurité était souvent vécue comme un sujet technique réservé aux informaticiens et responsable du système de sécurité informatique encore aujourd'hui, ça reste le cas. Les premières vagues de déploiement ont permis de faire émerger une nouvelle vision, celle d'un enjeu managérial et stratégique, né à la continuité des soins et à la confiance des patients. Les directions hospitalières se saisissent désormais plus volontiers de ces questions, ce qui amorce une transformation formatrice essentielle.

b) Le kit PCRA, un outil pragmatique et accessible

Le kit PCRA, même s'il reste à implémenter, propose une démarche structurée, compréhensible par des équipes aux compétences hétérogènes. Il rend visible la vulnérabilité réelle de certains processus comme la dépendance aux SI pour la gestion des urgences), tout en offrant des points d'appui concrets pour y remédier.

c) L'effet pédagogique des audits

Les audits techniques menés dans les établissements ont eu un impact pédagogique fort. Ils ont permis de briser le tabou que « les hôpitaux n'intéressent pas les cybercriminels ». Confrontés à des failles documentées, les soignants et les administratifs ont pu toucher du doigt la réalité des cyberattaques, et commencer à réfléchir collectivement aux mesures correctrices, bien au-delà de la simple technicité des RSSI.

3.2. Les faiblesses, résistances, inertie et disparités

a) Le manque de temps et de ressources humaines

La principale difficulté reste la surcharge chronique des équipes hospitalières. Dans un quotidien déjà marqué par la pression des soins, la crise des ressources humaines et la multiplication des exigences réglementaires, trouver le temps et l'énergie pour formaliser

un plan de continuité cyber est un véritable défi. Même si les directions reconnaissent l'importance de CaRE, sa mise en œuvre est souvent reportée ou réalisée a minima.

b) Une culturation insuffisamment mature

Bien que les directions soient désormais plus sensibilisées, l'acculturation au risque cyber reste encore insuffisante parmi les professionnels de terrain, qu'ils soient médicaux, administratifs ou techniques. Beaucoup d'entre eux continuent à percevoir la cybersécurité comme une contrainte supplémentaire imposée plutôt que comme une responsabilité collective nécessaire pour garantir la continuité et la sécurité des soins. Ce manque d'acculturation se traduit souvent par une appropriation superficielle des outils proposés, ce qui limite leur efficacité réelle en cas de crise.

c) Des écarts de maturité préoccupants

La mise en œuvre de CaRE révèle des écarts préoccupants entre les établissements. Les CHU et les grands centres disposent souvent d'équipes formées et de moyens financiers pour avancer rapidement. A l'inverse, les hôpitaux ruraux et les structures médico-sociales peinent à s'approprier les outils, faute de compétences internes et de moyens d'ingénierie. Cette fracture numérique hospitalière est un défi majeur pour l'égalité d'accès aux soins, même en cas de cybercrise.

4. Analyse comparative des forces de CaRE et des axes d'amélioration inspirés d'EBIOS

4.1. Les points forts de CaRE

L'un des atouts majeurs de CaRE est sa capacité à rendre la cybersécurité concrète pour les établissements. Grâce aux audits techniques, aux outils PCRA et au soutien des ARS, CaRE ancre la cybersécurité dans les réalités du terrain. Il a traduit en action concrète en binôme métiers-techniques, en formation et en mutualisation d'expériences. Cette approche progressive, articulée autour de la gouvernance et de la sensibilisation, est précieuse dans un secteur où les ressources sont limitées et les enjeux multiples.

Autre force, c'est la focalisation sur la continuité des soins. Là où beaucoup de démarches cyber se cantonnent à l'aspect technique, CaRE lie explicitement la sécurité des SI au

cœur de la mission hospitalière : soigner, même en situation de crise. Ce lien avec les soins est un puissant levier pour engager les équipes.

4.2. Les limites de CaRE

Cette focalisation sur la réponse opérationnelle laisse en suspens un aspect fondamental de la résilience, la capacité à anticiper les scénarios d'attaque et à comprendre la logique des adversaires. CaRE, tel qu'il est conçu aujourd'hui, ne propose pas de cadre structuré pour analyser les menaces et modéliser les attaques. Il se concentre sur la remédiation des vulnérabilités connues et sur l'organisation de la réponse, sans aborder en profondeur la préparation aux modes opératoires les plus récents et les plus sophistiqués.

Ce vide peut conduire à une certaine fragilité structurelle, un établissement qui a corrigé ses failles connues mais qui n'a pas pensé à la façon dont un attaquant pourrait les contourner reste vulnérable. La résilience, pour être complète, doit dépasser la simple remédiation pour inclure une compréhension active de l'adversaire.

4.3. Ce qu'EBIOS RM peut apporter

C'est précisément dans cette dimension qu'EBIOS RM trouve toute sa pertinence. Une méthodologie rigoureuse, elle permet d'aller au-delà de l'inventaire des vulnérabilités techniques pour :

- Identifier les actifs vitaux d'un hôpital ;
- Analyser les scénarios d'attaques crédibles, en tenant compte des motivations des attaquants et des modes opératoires émergents ;
- Prioriser les mesures de sécurité en fonction de l'impact métier et de la vraisemblance des menaces.

4.3. Une synergie à construire au service de la résilience réelle

Finalement, l'analyse croisée dessine une complémentarité stratégique :

- CaRE structure la réponse opérationnelle et la mise en place des outils de crise, indispensables pour la continuité des soins.
- EBIOS RM offre la capacité à anticiper, à comprendre les menaces et à prioriser les actions en profondeur.

Cette synergie est essentielle pour éviter que CaRE ne devienne un simple outil de conformité, ou qu'EBIOS RM ne reste une démarche élitiste, réservée à quelques établissements pilotes. Elle incarne l'idée même de la cybersécurité hospitalière moderne. Un pont entre la réalité du soin, l'impératif de réaction et l'intelligence de l'anticipation.

L'analyse du programme CaRE, mise en perspective avec la méthode EBIOS RM, montre que la résilience face aux cyberattaques ne peut reposer sur un seul levier. Elle nécessite une double approche, à la fois stratégique et opérationnelle, qui reste encore peu intégrée dans les pratiques hospitalières. Pour mieux comprendre comment ces outils sont réellement mobilisés sur le terrain, et dans quelle mesure ils influencent la gestion des crises cyber, il est désormais indispensable de croiser ces constats théoriques avec des retours d'expérience issus des établissements de santé eux-mêmes. C'est l'objet de la Partie IV.

PARTIE IV : TERRAIN ET RETOURS D'EXPÉRIENCE

1.Méthodologie de l'étude qualitative

a) Positionnement épistémologique

Cette étude qualitative adopte un positionnement épistémologique interprétatif. L'objectif est de comprendre en profondeur les perceptions, les expériences et les vécus des acteurs impliqués dans la gestion des cyber-risques au sein des établissements de santé. Plutôt que de chercher à généraliser des faits ou à établir des lois universelles, l'approche vise à saisir la complexité des situations, les nuances des discours et la richesse des contextes spécifiques. Cela implique une reconnaissance de la subjectivité des participants et une volonté d'explorer les significations qu'ils attribuent à leurs actions et aux dispositifs mis en place, tels qu'EBIOS et le programme CaRE.

1. 1. Méthodologie de collecte des données

La collecte des données s'est appuyée sur deux méthodes principales : les entretiens semi-directifs et l'analyse de webinaires de retours d'expérience.

a) Des entretiens semi-directifs

Cinq entretiens ont été menés avec des professionnels clés du secteur de la santé et de la cybersécurité. Cette méthode a permis d'explorer en détail les expériences individuelles, les opinions et les perceptions des participants, tout en laissant une certaine flexibilité pour aborder des thèmes émergents. Les entretiens ont été enregistrés et retranscrits intégralement pour une analyse approfondie.

Entretien	Fonction	Type d'établissement	Date	Durée
1	RSSI	Sanitaire	27/03/2025	43 min
2	Expert cyber&RSSI	Éditeur de la solution Agile Risk Manager intégrant EBIOS.	7/04/2025	31min
3	Coordonnateur SSE	Sanitaire, établissement pilote CaRE	23/04/2025	47 min

4	RSI	Sanitaire	29/04/2025	1h
5	Technicienne Informatique	Sanitaire	8/05/2025	54 min

Tableau 1 : professionnels ayant participé aux entretiens semi-directifs

b) Analyse de webinaires de retours d'expérience

Pour enrichir la perspective et compenser le nombre limité d'entretiens, des webinaires pertinents ont été consultés. Ces ressources ont offert des retours d'expérience complémentaires et des éclairages sur l'application d'EBIOS RM et du programme CaRE dans divers établissements de santé.

Webinaires sur la méthode EBIOS RM dans le secteur de la santé	La méthode EBIOS RM modélisée pour les établissements de santé [41]. Analyse de risques cyber - EBIOS RM à l'épreuve de l'hôpital et de ses partenaires [42].
Webinaires sur le programme CaRE et la gestion des cybercrises	Programme CaRE, Présentation des kits d'exercice de crise V2 [43]. Programme CaRE Atteinte des objectifs Domaine 1 - Questions fréquentes et points d'attention [44]. Programme CaRE du ministère de la Santé, Protéger les établissements de santé et répondre aux exigences du Domaine 1" (Specops Software / Outpost24, 17 septembre 2024) [45].

Tableau 2 : liste des webinaires

c) Échantillonnage

L'échantillonnage est de type intentionnel et s'est concentré sur des profils d'experts et de praticiens directement impliqués dans la cybersécurité et la gestion de crise au sein d'établissements de santé ou en tant que prestataires spécialisés. Le choix des participants a été guidé par leur connaissance approfondie d'EBIOS, du programme CaRE, ou de la gestion des risques cyber en milieu hospitalier. L'inclusion d'un CHU pilote du programme CaRE et d'un hôpital à Mayotte a permis d'obtenir des perspectives

variées, allant des structures les plus avancées aux plus contraintes en termes de ressources.

Étant notifié de l'anonymat dans mon travail, les interlocuteurs seront désignés par leur fonction.

d) Analyse des données

L'analyse repose sur une analyse thématique manuelle, suivant une démarche d'analyse de contenu mixte :

Les entretiens ont été retranscrits puis codés selon des unités de sens, à partir :

- Des objectifs de recherche
- Des dimensions explorées dans le guide d'entretien
- De l'analyse inductive des verbatims

Les webinaires ont été analysés de manière complémentaire, en relevant les points de convergence ou de divergence avec les témoignages recueillis. Cette triangulation a permis de renforcer la profondeur de l'analyse, en confrontant les pratiques réelles aux enseignements collectifs partagés à l'échelle nationale.

e) Limites de la méthodologie

Bien que rigoureuse, cette méthodologie présente certaines limites :

- Taille de l'échantillon : Le nombre limité d'entretiens (cinq) ne permet pas une généralisation statistique des résultats à l'ensemble des établissements de santé. L'étude est de nature qualitative et vise la profondeur plutôt que la représentativité quantitative.
- Subjectivité des participants : Les données collectées sont basées sur les perceptions et les expériences des individus, ce qui peut introduire un biais de subjectivité. L'analyse s'est efforcée de reconnaître et de contextualiser ces perspectives.
- Dépendance aux informations disponibles : L'analyse des webinaires dépend des informations publiquement disponibles, ce qui constitue une limitation méthodologique significative. En effet, dans le domaine de la cybersécurité, le caractère extrêmement sensible des informations relatives aux failles ou aux incidents fait que les acteurs ne divulguent souvent pas toutes les données par souci de confidentialité et de sécurité. « *Malheureusement, la transparence ne fait*

pas encore partie intégrante de la culture générale de la cybersécurité, hormis dans des contextes très spécifiques. Bien que des cadres comme le Règlement Général sur la Protection des Données (RGPD) tentent d'accroître cette transparence en imposant la déclaration des violations de données personnelles, cette obligation ne concerne pas tous les types d'incidents, laissant ainsi de nombreuses informations hors du domaine public et ne permettant pas d'interroger directement les intervenants pour des clarifications complètes. » [46].

- Spécificité du contexte hospitalier : Bien que l'étude se concentre sur les établissements de santé, les résultats peuvent ne pas être directement transposables à d'autres secteurs.
- Évolution rapide du domaine : La cybersécurité est un domaine en constante évolution, ce qui signifie que certaines informations ou observations peuvent devenir obsolètes rapidement.

1.2. Présentation des participants et des contextes

Cette section vise à introduire les profils des professionnels interrogés, en soulignant leur rôle spécifique et le contexte de leur établissement ou de leur activité, afin de mieux appréhender les perspectives et les retours d'expérience qui seront développés par la suite.

1) RSSI

Le premier entretien a été réalisé avec le RSSI (Responsable de la Sécurité des Systèmes d'Information) d'un CH hors territoire. Ce témoignage est essentiel car il représente la perspective d'un établissement situé dans un contexte géographique et structurel potentiellement différent de ceux de la métropole. L'établissement est confronté à des défis spécifiques, qui peuvent inclure des contraintes de ressources, des infrastructures particulières, ou une exposition à des menaces spécifiques. La vision de ce RSSI offre un éclairage sur la résilience cyber dans un environnement insulaire et sur l'adaptation des démarches nationales (comme EBIOS et CaRE) aux réalités locales. Son expérience met en lumière l'importance de la sensibilisation du personnel et de l'adaptation des outils aux environnements spécifiques.

2) Expert Cyber & RSSI de ALL4TEC

Le deuxième participant est un expert Cyber et RSSI (Responsable de la Sécurité des Systèmes d'Information) chez ALL4TEC, éditeur de la solution Agile Risk Manager

intégrant EBIOS. Il apporte une vision d'éditeur de solution et de prestataire de services spécialisé dans la méthode EBIOS RM. Son expertise couvre l'ensemble des aspects théoriques et pratiques de l'analyse de risques selon EBIOS, ainsi que son adaptation aux besoins spécifiques des clients, notamment dans le secteur de la santé. Son rôle permet de comprendre les enjeux de la modélisation des risques, l'automatisation des processus EBIOS, et la manière dont les établissements peuvent tirer le meilleur parti de cette méthode. Ses retours sont précieux pour comprendre les fondements et les évolutions d'EBIOS, ainsi que les difficultés courantes rencontrées par les utilisateurs.

3) Coordonnateur Situation Sanitaire Exceptionnelle (SSE)

Le troisième entretien a été mené avec le Coordonnateur de Situation Sanitaire Exceptionnelle (SSE) d'un CHU., faisant partie des structures pilote pour le domaine 2 CaRE. Ce profil est particulièrement pertinent car il se situe à l'interface entre la gestion des crises sanitaires générales et l'intégration des risques cyber dans cette démarche. Le CHU a bénéficié d'un accompagnement spécifique et d'une participation active dans le déploiement des outils et des exercices du programme CaRE. La perspective de ce coordonnateur offre un aperçu unique sur l'application concrète de CaRE, les défis rencontrés par un grand établissement hospitalier, et l'impact des exercices de crise sur la préparation opérationnelle. Sa position lui permet d'évaluer l'articulation entre la gestion des cyber-crises et les plans de continuité d'activité plus larges.

4) Responsable du Système d'Information (RSI)

Le quatrième participant est le Responsable du Système d'Information (RSI) d'un établissement de santé. Son rôle stratégique le place à la tête de la gestion globale de l'informatique et de la cybersécurité. En tant que RSI, il est responsable de la définition et de la mise en œuvre de la politique de sécurité des systèmes d'information (PSSI), de la coordination des équipes techniques et de la prise de décisions en matière d'investissements et de priorités. Sa perspective est celle d'un décideur confronté aux enjeux à la fois techniques, organisationnels, humains et budgétaires de la cybersécurité. Son expérience apporte un éclairage sur la gouvernance de la cybersécurité et l'intégration des démarches de gestion des risques à l'échelle de l'établissement.

5) Technicienne informatique

La cinquième participante est une technicienne au service informatique d'un établissement de santé. Avec cinq ans d'ancienneté dans l'établissement, dont plus de deux ans d'implication directe dans les questions de cybersécurité, elle est au cœur de la gestion quotidienne du système d'information. Son rôle englobe la gestion des postes et des serveurs, ainsi que la sécurité des accès et des données. Son expérience directe d'un incident de phishing sérieux il y a trois ans a renforcé sa conscience de l'importance d'une préparation rigoureuse et a mis en lumière la dimension non seulement technique mais aussi humaine de la gestion de crise. Elle est activement impliquée dans la mise en place du programme CaRE et la participation aux exercices de gestion de crise, ce qui lui

confère une perspective opérationnelle précieuse sur les défis et les bonnes pratiques en matière de cyber-résilience.

2.État des lieux de la gestion des cyber-risques dans les établissements de santé

En se basant sur les témoignages des professionnels interrogés et les retours d'expérience plus larges issus des webinaires, on analyse la situation actuelle de la gestion des cyber risques au sein des établissements de santé. La section aborde la perception de la menace, les mesures de prévention et de détection en place, l'utilisation d'outils génériques, et l'importance cruciale de la dimension humaine.

2.1. Conscience de la menace et fréquence des incidents

Les entretiens menés révèlent une conscience aiguë et généralisée de la menace cyber au sein des établissements de santé. Cette prise de conscience n'est plus théorique mais s'appuie sur des expériences concrètes ou sur la résonance des attaques médiatisées dans le secteur. La technicienne informatique témoigne d'un « *phishing bien ficelé qui avait failli passer* » il y a trois ans, un événement qui a profondément marqué l'établissement et renforcé sa vigilance. Cet incident a mis en lumière que « *la gestion de crise ne se limite pas à la technique* », soulignant l'importance de la réactivité et de la coordination au-delà des seuls aspects technologiques.

Le RSSI du CH corrobore cette observation en évoquant une « *augmentation des tentatives de cyberattaques* » comme une réalité quotidienne. Ces tentatives, qu'elles soient abouties ou non, contribuent à maintenir un niveau élevé de vigilance. Le Coordonnateur SSE, confirme la nécessité impérieuse de « *se préparer aux cyberattaques* », reconnaissant la « *réalité des menaces actuelles* » qui pèsent sur la continuité des soins et la protection des données. La médiatisation croissante des attaques contre des hôpitaux renforce cette perception, transformant une menace abstraite en un risque tangible et immédiat pour la mission de soin.

Bien que la fréquence exacte des incidents majeurs varie, l'ensemble des interlocuteurs s'accorde sur le caractère persistant et évolutif de la menace cyber. L'expert Cyber de ALL4TEC, du fait de sa position d'observateur privilégié du marché, confirme cette tendance générale à la hausse, expliquant que le secteur de la santé est une cible de

choix en raison de la sensibilité des données qu'il détient (données de santé personnelles) et de l'impact potentiellement catastrophique d'une interruption de service sur la vie des patients.

2.2. Mesures techniques de prévention et de détection existantes

Face à cette menace grandissante, les établissements de santé ont mis en place diverses mesures techniques visant à prévenir et détecter les cyber-risques. La technicienne informatique insiste sur l'importance d'une approche proactive, mentionnant explicitement la « *veille tous les jours sur les failles et les alertes* » et la « *mise à jour des cartographies et des analyses de risques régulièrement* ». Ces actions traduisent une tentative d'anticipation des vulnérabilités avant qu'elles ne soient exploitées.

Plus globalement, les RSSI interrogés, font référence à des « *outils de gestion des risques* », ce qui implique généralement un panel de solutions de sécurité informatique. Ces outils incluent des systèmes de détection et de prévention d'intrusions, des pares-feux de nouvelle génération, des antivirus et des solutions de protection, ainsi que des systèmes de gestion des vulnérabilités et d'analyse des logs de sécurité.

Cependant, les entretiens révèlent également que la mise en œuvre de ces mesures techniques n'est pas sans défis. Le Responsable du Système d'Information (RSI) souligne l'équilibre délicat entre « *les exigences de sécurité et les contraintes opérationnelles et budgétaires* ». Cette réalité budgétaire et la complexité des systèmes d'information hospitaliers peuvent parfois limiter l'étendue et la sophistication des outils de sécurité déployés, rendant la tâche ardue pour les équipes informatiques.

2.3. Utilisation et perception des outils et méthodes de gestion des risques (hors EBIOS et CaRE)

Avant l'intégration plus structurée de méthodes comme EBIOS et le programme CaRE, les établissements s'appuient sur des pratiques de gestion des risques plus génériques, souvent inspirées de cadres généraux ou de standards internationaux. Le RSI, par exemple, a la charge de la « *définition et la mise en œuvre de la politique de sécurité des*

systèmes d'information (PSSI) », qui constitue le document cadre pour la gestion des risques et des règles de sécurité au sein de l'établissement.

La technicienne informatique évoque la « *mise à jour cartographies et analyses de risques* », suggérant l'utilisation de méthodologies d'identification des actifs, d'évaluation des menaces et des vulnérabilités, et de calcul des risques résiduels. Ces approches, bien que fondamentales pour toute démarche de sécurité, sont parfois perçues comme moins spécifiquement adaptées aux nuances des cyber-risques ou comme manquant d'une granularité suffisante pour la prise de décision.

La perception générale est que, si ces outils génériques fournissent une base nécessaire, ils peuvent ne pas offrir la profondeur d'analyse ou la structure nécessaires pour traiter efficacement les risques cyber complexes et évolutifs du secteur de la santé. Cette lacune pousse les établissements à rechercher des méthodes plus spécialisées et des cadres d'action ciblés pour renforcer leur résilience.

2.4. La dimension humaine : sensibilisation et formation du personnel

Un point de convergence majeur dans tous les entretiens est l'importance capitale de la dimension humaine dans la gestion des cyber-risques. La technicienne informatique, ayant vécu un incident de phishing, affirme avec force que « *la gestion de crise ne se limite pas à la technique* » et que « *la première ligne de défense, c'est l'humain* ». Elle insiste sur la nécessité de « *sensibiliser le personnel avec des petites fiches pratiques et des formations* », soulignant que le comportement des utilisateurs est souvent le maillon faible de la chaîne de sécurité.

Le RSSI place la « *sensibilisation du personnel* » au rang des priorités absolues, conseillant de « *renforcer la sensibilisation du personnel et d'adapter les outils de gestion des risques à leur environnement spécifique* ». Il ajoute qu'il est impératif de « *continuer à sensibiliser et former le personnel* » pour faire face à la réalité des menaces. Le Coordonnateur SSE bien que son rôle soit axé sur CaRE, valide implicitement cette idée en évoquant les bénéfices des exercices pour la « *montée en compétence collective* », ce qui inclut la capacité des équipes à réagir humainement en situation de crise.

La gestion des cyber-risques est donc perçue comme un défi systémique, où la technologie doit impérativement être complétée par une culture de sécurité forte et une vigilance humaine constante.

3.Le programme CaRE à l'épreuve du terrain : Analyse de son impact sur la gestion des crises cyber

Ici, nous explorons la mesure dans laquelle le programme Cybersécurité Accélération et Résilience des Établissements permet aux établissements de santé de gérer les crises liées aux cyberattaques. Elle s'appuie sur les témoignages des participants, en particulier celui du Coordonnateur SSE du CHU pilote, et sur les informations issues des webinaires dédiés au programme CaRE

3.1. Déploiement et appropriation du programme CaRE

Le programme CaRE, initié par le ministère de la Santé, vise à renforcer la cyber-résilience des établissements de santé. Les entretiens révèlent des niveaux d'adoption et d'appropriation variés, mais une reconnaissance unanime de son utilité comme cadre structurant. La technicienne informatique est « *impliquée directement dans les questions de cybersécurité, notamment pour la mise en place du programme CaRE et des exercices de gestion de crise* », ce qui démontre un déploiement actif sur le terrain. Le Coordonnateur SSE, en tant qu'établissement pilote, a une connaissance du programme et en perçoit la valeur stratégique.

Les webinaires sur CaRE ("Programme CaRE - Présentation des kits d'exercice de crise V2" par l'ANS) confirment que le programme est activement poussé par l'Agence du Numérique en Santé et touche un nombre croissant d'établissements. L'adhésion des équipes dirigeantes et opérationnelles est un facteur clé de succès. Le RSSI, bien que confronté à des défis spécifiques, reconnaît l'importance des cadres nationaux comme CaRE pour orienter leurs efforts. Il est perçu comme une « *feuille de route* » permettant aux établissements de se conformer aux exigences et de monter en maturité.

3.2. Apports concrets de CaRE pour la gestion des crises cyber

Le programme CaRE est unanimement salué pour ses apports tangibles dans la préparation et la gestion des cyber-crises.

a) Structuration de la réponse à crise

L'un des bénéfices majeurs de CaRE est la formalisation et la structuration des processus de réponse à incident et de gestion de crise. Le Coordonnateur SSE souligne que le programme a permis de « *formaliser des procédures de gestion de crise cyber* », ce qui est essentiel pour une réaction rapide et coordonnée. Les kits d'exercices de crise (V2), présentés par l'ANS, fournissent des scénarios et des outils pour simuler des attaques, permettant aux équipes de s'entraîner à la mise en œuvre de cellules de crise, à la prise de décision en situation de stress et à la coordination interservices.

b) Montée en compétence collective

CaRE met un accent particulier sur la formation et les exercices pratiques, ce qui contribue directement à la « *montée en compétence collective* » des équipes. La technicienne informatique, en participant aux exercices, confirme que ces simulations sont cruciales pour que « *chacun sache quoi faire en cas d'attaque* ». Le webinaire de l'ANS sur les kits d'exercice met en avant les retours d'expérience de sept établissements pilotes, démontrant l'efficacité de cette approche pédagogique pour améliorer la réactivité et la coordination des acteurs impliqués (équipes informatiques, direction, communication, services de soins).

c) Renforcement des stratégies de continuité et de reprise d'activité (PCA/PRA)

Le Domaine 2 du programme CaRE, comme le montre le webinaire organisé par Orange Cyberdéfense (« Renforcer votre cyber résilience avec le Domaine 2 du programme CaRE »), est spécifiquement dédié à la stratégie de continuité et de reprise d'activité (PCA/PRA). Les témoignages d'établissements de santé dans ce webinaire illustrent comment CaRE pousse à une réflexion approfondie sur la résilience des infrastructures critiques et la capacité à restaurer les services après une cyberattaque. Ce volet est important pour limiter l'impact sur les soins et la prise en charge des patients.

d) Protection des systèmes et des données

Le Domaine 1 de CaRE, présenté par Specops Software / Outpost24 dans un webinaire dédié (« Programme CaRE du ministère de la Santé : Protéger les établissements de santé et répondre aux exigences du Domaine 1 »), se concentre sur la surveillance de l'exposition des établissements de santé sur Internet et la réduction de la surface d'attaque. Bien que plus orienté vers la prévention, ce domaine contribue indirectement à la gestion de crise en réduisant la probabilité et la gravité des incidents. La capacité à identifier et à corriger les vulnérabilités externes permet de mieux « *protéger les établissements de santé* » en amont, diminuant ainsi le risque de devoir gérer une crise majeure.

e) Témoignage sur la capacité à réagir et à se coordonner

Globalement, les participants perçoivent un renforcement de leur capacité à réagir et à se coordonner. Le Coordonnateur évoque une meilleure « *préparation opérationnelle* » et une

plus grande fluidité dans la communication interne et externe lors des simulations de crise. La technicienne informatique, confrontée à un incident réel par le passé, perçoit CaRE comme un levier pour éviter qu'un tel événement ne dégénère en crise ingérable, grâce à la mise en place de réflexes et de procédures claires.

3.3. Défis et limites du programme CaRE

Malgré ses apports avérés, le déploiement et la pleine exploitation du programme CaRE rencontrent plusieurs défis.

a) Contraintes de ressources (humaines, financières) pour le déploiement

Le RSSI met en évidence les “*contraintes budgétaires*" et le manque de "*ressources humaines spécialisées*" comme des freins majeurs à l'application optimale des recommandations de CaRE. Pour de nombreux établissements, surtout les plus petits ou ceux avec des budgets limités, allouer du personnel et des fonds spécifiquement à la cybersécurité et aux exercices peut être un défi.

b) Difficultés d’intégration avec les processus existants

L'intégration des nouvelles procédures et exigences de CaRE avec les processus de gestion de crise et les plans d'urgence déjà existants (plan blanc, plan de continuité d'activité général) peut s'avérer complexe. Le Coordonnateur mentionne la nécessité d'une « *harmonisation des procédures* » pour éviter les redondances ou les incohérences, ce qui demande un travail de coordination significatif.

c) Besoins d'adaptation à la taille et aux spécificités de chaque établissement

Le programme CaRE, bien que national, doit être adapté à la diversité des établissements de santé (taille, niveau de ressources, spécificités géographiques). Le RSSI, par exemple, souligne qu'il vaudrait « *mieux adapter les outils de gestion des risques à la réalité des établissements de santé* », ce qui s'applique aussi aux exercices de CaRE. Les scénarios doivent être pertinents et proportionnés aux capacités de chaque structure pour être efficaces.

d) La question de la pérennisation des efforts au-delà des exercices

Enfin, un défi récurrent est la pérennisation des efforts de préparation et de formation. Une fois les exercices terminés, il est capital de maintenir le niveau de compétence et la vigilance. La technicienne informatique insiste sur le fait que la cybersécurité est un « *réflexe maintenant* », mais cela nécessite une « *veille continue* » et des rappels réguliers pour éviter un relâchement après la phase initiale de mise en œuvre de CaRE. La fréquence et la qualité des exercices de maintien en condition opérationnelle sont donc essentielles.

4.La méthode EBIOS : levier pour renforcer la résilience

Cette section explore dans quelle mesure la méthode Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager (EBIOS RM), constitue un enseignement précieux pour renforcer la résilience des établissements de santé face aux cyberattaques. Elle s'appuie sur les retours d'expérience des webinaires spécifiquement dédiés à l'application d'EBIOS RM dans le secteur de la santé.

4.1. Connaissance et adoption d'EBIOS RM dans le secteur de la santé

La connaissance et l'adoption d'EBIOS RM par les établissements de santé sont un sujet nuancé. Si la méthode est reconnue comme une référence par les experts, son déploiement effectif sur le terrain peut varier. Les webinaires sur EBIOS RM dans le secteur de la santé (« La méthode EBIOS RM modélisée pour les établissements de santé », ou « Analyse de risques cyber – EBIOS RM à l'épreuve de l'hôpital et de ses partenaires ») mettent en évidence l'intérêt croissant pour son application spécifique au contexte hospitalier. Le CHU de Toulouse, cité dans le premier webinaire, est un exemple d'établissement ayant adapté EBIOS RM, démontrant qu'il est possible de l'intégrer avec succès dans un environnement complexe.

Cependant, il est également mentionné que « *la complexité perçue de la méthode* » peut être un frein à son adoption généralisée sans accompagnement. La technicienne informatique et les RSSI de petits établissements peuvent ne pas maîtriser EBIOS en profondeur, soulignant un écart potentiel entre la reconnaissance de l'outil par les experts et sa pleine intégration opérationnelle.

4.2. Contributions d'EBIOS à la compréhension et à la maîtrise des risques

EBIOS RM est présenté comme un outil puissant pour une compréhension approfondie et une meilleure maîtrise des risques cyber, éléments fondamentaux pour la résilience.

a) Identification et analyse approfondie des menaces et vulnérabilités

La force d'EBIOS réside dans sa capacité à permettre une « *analyse fine des risques* ». La méthode guide les utilisateurs pour identifier de manière exhaustive les actifs critiques, les sources de menaces, les vulnérabilités associées et les événements redoutés. Cette approche systématique garantit qu'aucun aspect important du système d'information n'est négligé dans l'évaluation des risques. Pour les établissements de santé, cela signifie une meilleure compréhension des points faibles spécifiques aux systèmes de soins, aux dispositifs médicaux connectés et aux données patientes. « Cette analyse fine des risques est également primordiale pour vérifier si ces risques sont bien couverts par les mesures mises en place dans un programme comme CaRE ».

b) Définition de scénarios de risque

EBIOS RM encourage la « *définition de scénarios de risque* » qu'ils soient stratégiques ou opérationnels. Ces scénarios permettent de se projeter dans des situations concrètes d'attaques, aidant ainsi à comprendre les vecteurs d'attaque potentiels, les objectifs des attaquants et les impacts prévus. Cette capacité à imaginer et à modéliser différents types d'attaques (par exemple, rançongiciel, compromission de données patients, paralysie d'un service d'urgence) est un enseignement majeur pour la préparation aux crises. En identifiant les scénarios les plus critiques, les établissements peuvent concentrer leurs efforts de protection et de réponse.

c) Évaluation de la couverture des mesures de sécurité existantes

La méthode EBIOS permet également d'évaluer l'efficacité des mesures de sécurité déjà en place par rapport aux scénarios de risques identifiés. Elle aide à déterminer si les contrôles techniques et organisationnels actuels sont suffisants ou s'il existe des lacunes à combler. Cette étape est en fait l'inverse de l'identification initiale des risques, car elle évalue dans quelle mesure les risques connus sont effectivement adressés par les dispositifs existants. Cette évaluation objective est cruciale pour identifier les priorités

d'investissement et pour s'assurer que les efforts de sécurité sont dirigés vers les risques les plus pertinents. Elle permet de créer un lien direct et de vérifier la cohérence entre l'analyse des risques en amont (via EBIOS) et l'implémentation des mesures en aval (comme celles du programme CaRE), constituant ainsi un outil d'évaluation de la cohérence globale de la stratégie de cybersécurité.

d) Aide à la décision et à la priorisation des investissements de sécurité

En quantifiant (même qualitativement) l'impact et la vraisemblance des risques, EBIOS RM fournit des éléments tangibles pour aider à la décision et à la priorisation des investissements en cybersécurité. Les résultats d'une analyse EBIOS peuvent être présentés à la direction pour justifier des budgets supplémentaires ou orienter les choix technologiques et organisationnels, en démontrant les gains en termes de réduction des risques. L'expert ALL4TEC insiste sur le fait qu'EBIOS aide à « *communiquer les risques de manière claire* » aux décideurs non techniques.

4.3. Défis et opportunités d'EBIOS pour les établissements de santé

L'adoption et l'exploitation d'EBIOS en milieu hospitalier présentent des défis mais aussi des opportunités significatives.

a) Complexité perçue de la méthode et besoin d'expertise

Le principal défi mentionné est la « *complexité perçue de la méthode* » EBIOS RM. Sa rigueur et sa profondeur nécessitent une certaine expertise et un investissement en temps pour être correctement mise en œuvre. De nombreux établissements de santé ne disposent pas toujours en interne de RSSI ou d'analystes de risques ayant une maîtrise suffisante d'EBIOS. Cela peut nécessiter le recours à des prestataires externes ou à des formations spécifiques.

b) Intégration des résultats d'EBIOS dans les plans d'action opérationnels

Un autre défi est de transformer les résultats de l'analyse EBIOS (qui est une démarche d'évaluation) en plans d'action concrets et opérationnels. Il ne suffit pas d'identifier les risques, il faut ensuite les traiter par des mesures techniques, organisationnelles ou

humaines. Le webinaire « Analyse de risques cyber-EBIOS RM à l'épreuve de l'hôpital et de ses partenaires » aborde cette problématique en discutant des défis de l'application d'EBIOS RM et de l'intégration de ses conclusions dans les stratégies de sécurité quotidiennes.

c) Retour d'expérience sur l'adaptation d'EBIOS au contexte hospitalier

L'adaptation de la méthode EBIOS RM au contexte hospitalier est une opportunité majeure. Le webinaire « La méthode EBIOS RM modélisée pour les établissements de santé » démontre que c'est possible et pertinent. Cela implique de prendre en compte les spécificités des SI hospitaliers (dispositifs médicaux, systèmes d'information patient, urgence des services), les contraintes réglementaires (RGPD, HDS) et la culture propre au monde de la santé. Des outils et des guides spécifiques peuvent faciliter cette adaptation.

d) EBIOS comme outil de sensibilisation interne et de dialogue avec la direction

Au-delà de l'analyse technique, EBIOS offre une opportunité de dialogue et de sensibilisation. En modélisant les scénarios d'attaques et leurs impacts potentiels sur l'activité des soins, la méthode permet de communiquer les risques de manière concrète à la direction et aux services métiers. Cette sensibilisation est nécessaire pour obtenir l'engagement de la gouvernance et des équipes non techniques, transformant ainsi la cybersécurité d'une affaire technique en un enjeu stratégique partagé par l'ensemble de l'établissement. EBIOS est un « *outil de communication* » essentiel pour « *faire passer le message* » et obtenir les ressources nécessaires.

5. Synergie et complémentarité perçues entre EBIOS et CaRE

Cette section analyse la manière dont les professionnels interrogés et les retours d'expérience issus des webinaires perçoivent l'articulation et la complémentarité entre la méthode EBIOS RM et le programme CaRE. Elle explore comment ces deux cadres, bien que distincts dans leur nature, peuvent se renforcer mutuellement sur le terrain pour améliorer la cyber-résilience des établissements de santé.

5.1. Comment l'approche par les risques d'EBIOS affine la préparation CaRE

Au-delà de la simple fourniture de scénarios, l'approche même d'EBIOS, qui met l'accent sur la compréhension des impacts et la priorisation des risques, est perçue comme essentielle pour affiner la préparation CaRE. En permettant une “*analyse fine des risques*", EBIOS aide à identifier les "*points de douleur*" spécifiques de l'établissement. Cela signifie que les efforts de préparation dans le cadre de CaRE peuvent être dirigés de manière plus stratégique vers les menaces les plus probables et les plus impactantes.

Le RSSI, bien qu'il n'ait pas explicitement mentionné EBIOS, a insisté sur la nécessité “*d’adapter les outils de gestion des risques à leur environnement spécifique*". EBIOS offre précisément cette capacité d'adaptation en contextualisant les risques. Ainsi, les ressources limitées disponibles pour CaRE peuvent être optimisées en se concentrant sur la résilience face aux risques les plus critiques identifiés par EBIOS, par exemple, en formant spécifiquement le personnel à des procédures de repli pour les services les plus vitaux en cas d'attaque par déni de service.

5.2. La perception d'une complémentarité entre l'analyse et l'entraînement

Globalement, la perception est que EBIOS et CaRE ne sont pas des doublons mais des étapes complémentaires dans un cycle vertueux de gestion des risques. CaRE, avec ses exercices et ses kits, est perçu comme la phase « *d'entraînement* » et de « *validation opérationnelle* » qui permet de tester la réactivité et la coordination des équipes face aux scénarios envisagés.

Les webinaires sur EBIOS RM et CaRE, bien que distincts, convergent vers l'idée que la meilleure préparation combine une compréhension théorique des risques avec une mise en pratique régulière des procédures de réponse. Cette synergie permet d'éviter que l'analyse de risques ne reste lettre morte et que les exercices ne se fassent sans une base de scénarios réalistes et priorisés. La technicienne informatique, confrontée à un incident réel par le passé, comprend l'intérêt de disposer d'une base solide pour la gestion de crise, ce que la formalisation des risques via EBIOS pourrait renforcer en amont de la mise en œuvre de CaRE.

5.3. Facteur facilitant ou freinant cette synergie sur le terrain

Bien que la complémentarité soit perçue, sa mise en œuvre sur le terrain peut être confrontée à des défis.

a) Facteurs facilitants

La présence d'un RSSI ayant une double compétence en analyse de risques et en gestion de crise, des outils logiciels qui intègrent les deux démarches (comme la solution Agile Risk Manager de ALL4TEC), ou une volonté managériale forte d'intégrer la cybersécurité dans une démarche qualité globale. La “*collaboration avec d'autres établissements*" évoquée par le RSSI de Mayotte pourrait également permettre le partage d'outils et de retours d'expérience sur l'articulation EBIOS-CaRE.

b) Facteurs freinant

Le manque de ressources humaines formées aux deux méthodes, la perception d'EBIOS comme une méthode trop complexe ou chronophage pour des établissements déjà sous contrainte, ou un cloisonnement entre les équipes chargées de l'analyse des risques et celles dédiées à la gestion de crise. Le défi réside souvent dans la traduction des résultats de l'analyse EBIOS en actions claires et intelligibles pour les équipes opérationnelles de CaRE, et inversement.

Pour conclure, la synergie entre EBIOS et CaRE est un levier puissant pour la cyber-résilience des établissements de santé. EBIOS fournit le "quoi" et le "pourquoi" des risques, tandis que CaRE permet de tester le "comment" de la réponse. La pleine exploitation de cette complémentarité nécessite une approche intégrée, des ressources adaptées et une volonté managériale de dépasser les cloisonnements pour une gestion des risques cyber à la fois approfondie et opérationnelle.

PARTIE V : PRÉCONISATIONS STRATÉGIQUES POUR UNE CYBERSÉCURITÉ INTÉGRÉE

1. Des cadres nationaux à la résilience

Dans un paysage sanitaire de plus en plus numérisé, la cyber-résilience n'est plus une simple option technologique, mais une composante indissociable de la sécurité des patients et de la continuité des soins. L'étude menée a mis en lumière la pertinence de deux cadres nationaux, la méthode EBIOS Risk Manager (EBIOS RM) et le programme Cybersécurité Accélération et Résilience des Établissements (CaRE), comme des piliers complémentaires pour structurer cette résilience. Loin d'être de simples outils informatiques, ils se révèlent être de véritables leviers managériaux pour intégrer la cybersécurité dans une gestion globale et proactive des risques en santé.

a) Complémentarité pour une approche globale des risques

L'analyse de risques avec EBIOS RM, telle que nous l'avons explorée, offre bien plus qu'une simple liste de vulnérabilités techniques. Elle permet une compréhension profonde des impacts potentiels sur les processus de soins et la qualité des données patients. C'est une démarche qui invite les managers à se poser des questions fondamentales : comment une cyberattaque pourrait-elle perturber la prise en charge d'un patient aux urgences ? Quels services vitaux seraient paralysés, et avec quelles conséquences directes sur la sécurité et le parcours de soin ? En identifiant ces scénarios, EBIOS fournit une cartographie des risques qui va au-delà du serveur ou du réseau pour toucher directement à la mission de l'établissement. Elle permet ainsi d'éclairer la prise de décision sur les priorités d'investissement et de protection, non pas en fonction de la complexité technique, mais de la criticité des processus pour la vie du patient.

En parallèle, le programme CaRE, avec ses kits d'exercices et sa dimension d'entraînement, prend le relais de cette réflexion amont. Il transforme l'analyse statique des risques en une préparation opérationnelle dynamique. Comme l'ont souligné les professionnels interrogés, CaRE permet de tester la capacité des équipes pluridisciplinaires, des soignants aux administrateurs, en passant par le personnel informatique à réagir collectivement. Il ne s'agit plus seulement de savoir ce qui peut arriver, mais bien comment y faire face. Les exercices de crise sont de véritables laboratoires où la coordination des flux (patients, informations, logistique), la gestion du

mode dégradé et la communication interne/externe sont mises à l'épreuve. C'est l'occasion de révéler les points de friction organisationnels et de renforcer les automatismes nécessaires en situation de stress.

b) L'intégration des risques cyber dans le management de la qualité des soins

La véritable force de la synergie entre EBIOS et CaRE réside dans leur capacité à transformer l'abstrait des cyber-risques en des enjeux concrets pour le management des flux et de la qualité des soins. Les scénarios modélisés par EBIOS, par exemple l'interruption des systèmes d'ordonnancement en pharmacie ou la perte d'accès aux dossiers patients informatisés, deviennent les points de départ d'exercices CaRE. Ces simulations permettent d'évaluer non seulement la capacité de l'IT à restaurer les systèmes, mais surtout celle de l'établissement à maintenir la qualité des soins et la sécurité des patients malgré la perturbation. Comment les flux de patients sont-ils réorganisés ? Les informations vitales sont-elles accessibles ? Le personnel soignant sait-il basculer en mode manuel en toute sécurité ?

C'est dans cette intégration que la cyber-résilience passe du domaine de l'informatique à celui du management stratégique des risques. Pour un manager des risques, ces outils offrent la possibilité d'anticiper les ruptures de parcours de soin et d'élaborer des plans de continuité d'activité qui ne sont pas de simples documents techniques, mais de véritables guides opérationnels pour préserver la qualité et la fluidité des services. La technicienne informatique soulignait d'ailleurs que la gestion de crise dépasse la technique, une observation qui résonne pleinement avec une approche managériale.

c) Un cadre national structurant au service de la performance organisationnelle

L'existence de cadres nationaux comme EBIOS et CaRE est un atout majeur pour les établissements de santé. Ils fournissent une feuille de route claire et des référentiels partagés, permettant aux hôpitaux, quelles que soient leur taille ou leurs ressources, de professionnaliser leur approche de la cybersécurité. Ces initiatives contribuent à élever le niveau de maturité cyber de l'ensemble du secteur, favorisant ainsi une meilleure coordination en cas de crise majeure touchant plusieurs établissements. Ils traduisent une volonté des autorités de transformer la cybersécurité d'une contrainte réglementaire en un

levier d'amélioration continue et de performance organisationnelle durable. En adoptant ces cadres, les établissements peuvent non seulement mieux se défendre, mais aussi rationaliser leurs investissements et optimiser leurs processus.

d) L'humain et l'organisation au cœur de la résilience

Finalement, EBIOS et CaRE, ensemble, rappellent avec force que la cyber-résilience est avant tout une affaire humaine et organisationnelle. Aucune technologie, aussi sophistiquée soit-elle, ne peut pallier l'absence de sensibilisation, de formation ou de coordination des équipes. La synergie de ces deux cadres met en lumière la nécessité d'un engagement managérial fort, d'une collaboration décloisonnée entre les services (IT, soignants, direction, qualité), et d'une culture de la sécurité partagée par chaque membre du personnel. C'est en faisant de la cybersécurité une préoccupation collective, intégrée dans le quotidien et les réflexes professionnels, que les établissements de santé pourront véritablement renforcer leur capacité à traverser les cyber-tempêtes, garantissant ainsi la pérennité de leur mission de soin et la sécurité des patients.

2. Recommandations concrètes pour les établissements

Les établissements de santé font face à une tension permanente entre des ressources limitées et des cybermenaces en constante évolution. Pourtant, des leviers d'action concrets, pragmatiques et accessibles existent pour renforcer leur résilience. À partir des constats issus des entretiens, de rapports spécialisés [46] et des analyses sectorielles, trois grands axes de recommandations se dégagent : managérial, opérationnel et pédagogique.

2.1. Recommandations managériales : faire de la cybersécurité une priorité stratégique et transversale

L'un des premiers leviers identifiés est de sortir la cybersécurité de sa zone "technique" pour l'inscrire dans la stratégie globale de l'établissement. Cela implique plusieurs actions structurantes :

- Nommer un référent cybersécurité transversal, rattaché à la direction ou à la coordination des risques, et pas uniquement à la DSI. Cette personne jouerait un

rôle de courroie de transmission entre les services. Dans le deuxième domaine de CaRE, il est attendu du PCRA, un responsable du système de management de la continuité d'activité (RSMCA). Ce qui rejoint fortement la recommandation sur le référent transversal. (Voir R1 : Désigner un responsable de la cybersécurité dans le guide de l'ANSSI).

- Intégrer le risque cyber à la cartographie globale des risques de l'établissement, au même titre que les risques sanitaires, logistiques ou humains. Cela permet de décloisonner les analyses et d'aligner les priorités avec les processus critiques réels. (Voir R2 : Intégrer la cybersécurité à la gouvernance et à la gestion des risques dans le guide de l'ANSSI).
- Intégrer à la cellule de gestion de crise le référent cybersécurité. Trop souvent, les plans de crise sur le volet numérique sont conçus par les informaticiens sans concertation avec les métiers. Or, une crise cyber affecte tous les niveaux de l'hôpital. (Voir R3 : Élaborer un plan de gestion de crise cyber dans le guide de l'ANSSI).
- Mobiliser la gouvernance (direction générale, CME, CSIRMT) autour de scénarios réalistes. Les entretiens montrent qu'un engagement fort de la direction est un facteur clé d'appropriation. (Voir R4 : Sensibiliser et former la gouvernance aux enjeux de la cybersécurité dans le guide de l'ANSSI).

2.2. Recommandations opérationnelles

Au-delà de la stratégie, des mesures concrètes et opérationnelles doivent être mises en place, même progressivement, pour renforcer la sécurité quotidienne des systèmes d'information et la capacité de réaction en cas de crise.

a) Gestion des Actifs et Analyse des Risques

L'établissement d'une base solide commence par une meilleure connaissance de son propre environnement.

Élaboration et maintien d'un registre d'actifs numériques à jour : comme le recommande Serge Houtain [36], cet inventaire est indispensable pour identifier les points faibles, les interdépendances, et les priorités en cas d'attaque. Ce registre doit être partagé entre les équipes métiers et techniques. (Voir R5 : Réaliser un inventaire précis des systèmes

d'information et des données critiques dans le guide de l'ANSSI).

Utilisation d'EBIOS en version allégée (analyse flash) pour identifier rapidement les scénarios de menace pertinents. Il est possible de mener ce type d'analyse d'un à deux jours, en ciblant quelques processus critiques. (Voir R6 : Mener des analyses de risques régulières dans le guide de l'ANSSI).

b) Renforcement de la Continuité et de la Résilience Opérationnelle

Adaptation des PCA/PRA à la réalité du terrain : trop souvent, ces plans sont génériques et inexploitables en cas de crise. Une mise à jour régulière, ancrée sur les scénarios identifiés par EBIOS, est essentielle. Le domaine 2 de CaRE met en avant l'analyse des scénarios d'indisponibilité tels que :

- Scénario "Perte des SI" : l'indisponibilité des logiciels et outils informatiques ;
- Scénario "Compétences" : indisponibilité du personnel et des compétences-clés ;
- Scénario "Bâtiment" : indisponibilité des locaux (incendie, rupture de fluides…) ;
- Scénario "Fournisseurs" : défaillance de fournisseurs directs.

Ces scénarios permettent l'identification des solutions de continuité et de reprise d'activité. (Voir R7 : Mettre en œuvre des plans de continuité et de reprise d'activité adaptés dans le guide de l'ANSSI).

Réalisation d'exercices de crise réguliers (simulation) avec le domaine 1 de CaRE, en intégrant l'ensemble des fonctions concernées. Ces exercices sont l'occasion de tester les chaînes de décision, la communication, et la capacité de maintien d'activité en situation dégradée. (Voir R8 : Tester régulièrement les plans de gestion de crise dans le guide de l'ANSSI).

Il est important de reconnaître que la mise en œuvre de ces exercices représente un investissement significatif en termes de coûts (ressources dédiées, outils de simulation) et peut entraîner une perturbation temporaire des activités courantes. Cependant, cet investissement est crucial pour valider l'efficacité des plans et réduire le coût potentiel d'un incident réel, souvent bien supérieur.

c) Mesures Techniques et Organisationnelles Fondamentales

Enfin, les fondations techniques doivent être solidement établies et intégrées dans une approche organisationnelle cohérente.

La mise à jour des équipements, le renforcement de la gestion des accès sont des mesures techniques classiques qui doivent être couplées à une approche organisationnelle claire pour être pleinement efficaces. (Voir R9 : Appliquer les mesures d'hygiène numérique fondamentales et R10 : Sécuriser les accès aux systèmes d'information dans le guide de l'ANSSI).

2.3. Recommandations en formation et sensibilisation

a) La cybersécurité en santé : Priorité aux systèmes, pas seulement aux utilisateurs

La gestion des cyber-crises dans les hôpitaux dépend moins des outils techniques que de la façon dont les systèmes sont conçus. Contrairement à une idée répandue, sensibiliser les employés à détecter chaque menace ne suffit pas. Bruce Schneier, expert en cybersécurité, explique qu'il est irréaliste d'attendre des utilisateurs qu'ils soient infaillibles face à des attaques de plus en plus complexes [47].

Le problème ne vient pas des utilisateurs qui commettraient des erreurs, mais de systèmes informatiques qui sont mal conçus et trop dépendants de la vigilance humaine. Se concentrer sur les erreurs individuelles détourne l'attention des faiblesses structurelles de la sécurité.

Pour une meilleure cyber-résilience, il faut donc des systèmes plus robustes (mises à jour automatiques, logiciels isolés, interfaces claires) qui réduisent les risques d'erreur. L'objectif est de concevoir la sécurité pour qu'elle fonctionne avec ou malgré le comportement humain, et non de blâmer les utilisateurs [48].

b) Doter l'Ensemble du Personnel des Réflexes de Base

Il est primordial de doter l'ensemble du personnel des réflexes de cybersécurité de base. Cela inclut la vigilance face au phishing, une gestion rigoureuse des mots de passe, ou encore l'utilisation sécurisée des supports de stockage. Ces formations doivent impérativement être adaptées aux réalités de chaque métier, qu'il s'agisse des soignants en première ligne de la prise en charge patient, du personnel administratif gérant des données sensibles, ou des cadres supervisant les opérations. (Voir R11 : Sensibiliser et former l'ensemble du personnel dans le guide de l'ANSSI).

c) Sensibilisation Ciblée des Cadres et Implication des Équipes

Parallèlement, la sensibilisation des cadres et responsables de service doit être ciblée et concrète. Il s'agit de leur faire percevoir les conséquences directes et souvent dramatiques d'un blocage du système d'information sur la continuité des soins, la sécurité des patients et la fluidité des flux opérationnels. C'est en impliquant activement les équipes soignantes dans des scénarios de crise, et en valorisant leur rôle indispensable dans la chaîne de résilience, à l'image des démarches initiées par des outils comme le Bilan d'Impact d'Activité (BIA) du programme CaRE, que l'on transforme la compréhension des risques en véritable engagement. Ce BIA, en caractérisant la criticité des activités et leurs interdépendances, permet de co-construire des solutions de continuité qui intègrent la perspective de l'ensemble du personnel, par le dialogue et la prise en compte de l'expérience terrain.

d) Simplification de la Communication et Formations Croisées

Pour que ces messages portent, la communication doit être simplifiée et accessible. L'élaboration de fiches réflexes, d'affiches concises ou de vidéos courtes permet de "descendre" la cybersécurité au plus près du terrain, dépouillée de tout jargon technique superflu. Enfin, il est crucial d'encourager les formations croisées entre la Direction des Systèmes d'Information (DSI), les équipes qualité, et les équipes de soins. Cette approche favorise une compréhension mutuelle des enjeux, des contraintes et des responsabilités de chacun, renforçant ainsi la cohésion et l'efficacité de la réponse collective en cas de cyber-incident.

e) Conclusion des recommandations

Ces recommandations, nourries par les réalités du terrain et les expertises reconnues, esquissent une cybersécurité intégrée, évolutive et partagée. Elles ne requièrent pas nécessairement des investissements colossaux. Le plus souvent, leur mise en œuvre dépend de choix de gouvernance clairs, d'une meilleure coordination interservices et d'une montée en compétence progressive. L'objectif n'est pas d'atteindre une perfection illusoire, mais d'engager une dynamique réaliste et cohérente avec les ressources et les priorités fondamentales des établissements de santé.

3. Perspectives : vers une culture de la cybersécurité en santé

Au fil des échanges et des analyses, un constat revient avec insistance : la cybersécurité ne peut plus être pensée comme un enjeu purement technique, ni comme une responsabilité exclusive de la DSI. Elle touche aujourd'hui l'ensemble du fonctionnement hospitalier, des soins à la logistique, de l'administration aux patients eux-mêmes. Il est donc nécessaire de dépasser la logique du "protocole en cas d'incident" pour entrer dans celle d'une véritable culture partagée de la cybersécurité.

Cette culture ne se décrète pas. Elle se construit, progressivement, à travers les comportements, les réflexes, les échanges entre les équipes, et l'attention portée aux signaux faibles. Elle repose aussi sur une meilleure lisibilité du risque, ce qui implique de traduire les enjeux techniques en conséquence concrètes pour les métiers. C'est précisément ce que permet la méthode EBIOS lorsqu'elle est bien adaptée : relier un scénario de menace à un processus de soins, à une rupture d'accès aux données, à une incapacité de facturer ou de tracer une transfusion.

Construire cette culture, c'est également rendre visible et légitime la cybersécurité dans tous les projets. Trop souvent, elle est perçue comme une contrainte, un ajout technique "en plus". Elle doit au contraire être pensée dès l'amont, dans les choix logiciels, dans les achats de dispositifs médicaux, dans la planification des formations ou des audits internes. Cela suppose une acculturation progressive de tous les professionnels, avec des messages adaptés, des exemples concrets et des approches qui respectent les contraintes réelles des services hospitaliers.

Les hôpitaux qui avancent sur cette voie montrent qu'il est possible de combiner des actions simples (fiches réflexes, analyses flash, formations ciblées) à des stratégies plus longues (gouvernance transversale, exercices pluridisciplinaires, usage structuré d'outils comme CaRE et EBIOS). Les témoignages issus des entretiens illustrent bien cette dynamique : il ne s'agit pas d'atteindre un niveau de maturité "idéal", mais d'évoluer pas à pas vers une approche plus préventive, coordonnée et impliquante.

Enfin, cette culture de la cybersécurité suppose aussi de s'autoriser à parler des échecs :

reconnaître les failles, analyser les incidents, capitaliser sur les crises. C'est le principe même de la résilience. À ce titre, les retours d'expérience (RETEX), les échanges entre établissements, et le soutien des agences nationales comme l'ANS ou l'ANSSI sont essentiels pour créer un environnement de confiance, d'entraide et d'amélioration continue.

Dans un monde hospitalier de plus en plus numérique, connecté, interdépendant, l'enjeu n'est plus de savoir si une attaque surviendra, mais dans quelle mesure l'établissement sera capable d'y faire face, d'en limiter les impacts et d'en sortir renforcé. C'est tout l'enjeu d'une culture de la cybersécurité intégrée à la mission même du soin.

4.Limites de l'étude et pistes de recherche futures

Ce mémoire a permis d'éclairer concrètement les enjeux et les pratiques actuelles de la cybersécurité dans les établissements de santé, en se plaçant sous l'angle du management des risques. Néanmoins, comme toute recherche, il est essentiel d'en souligner les limites, qui ne diminuent en rien la valeur de l'analyse, mais offrent des perspectives pour de futures recherches encore plus approfondies et complètes.

4.1. Limites de la présente étude

a) Le caractère récent des cadres et outils étudiés et le manque de recul opérationnel

Un facteur majeur circonscrivant la portée de cette étude est le caractère très récent des dispositifs au cœur de l'analyse. Le programme Cybersécurité Accélération et Résilience des Établissements (CaRE) est une initiative très récente et en constante évolution, tout comme l'application spécifique de la méthode EBIOS RM dans le domaine médical qui fait l'objet de mises à jour régulières. Cette jeunesse et cette dynamique des référentiels ont des implications directes.

Premièrement, l'appropriation de ces outils et référentiels sur le terrain est un processus continu, ce qui signifie que les pratiques observées au moment de l'étude sont susceptibles d'évoluer rapidement et de conférer à cette analyse une dimension contextuelle et temporelle spécifique.

Deuxièmement, le faible recul opérationnel et le nombre encore limité d'établissements ayant une expérience suffisamment avancée et documentée dans la mise en œuvre complète et le retour d'expérience de ces deux outils ont directement limité la quantité et la profondeur des informations empiriques disponibles. Le travail a donc dû s'appuyer davantage sur les cadres théoriques, les retours d'experts et les premières initiatives, plutôt que sur une multitude d'exemples de déploiements matures et de résultats tangibles.

b) Les contraintes liées à la collecte de données empiriques

La nature spécifique du sujet a également influencé la collecte de données :

- **Disponibilité limitée de ressources spécialisées :**

La recherche documentaire a révélé un champ de littérature académique encore peu fourni et fragmenté spécifiquement sur la cybersécurité appliquée au secteur de la santé, en particulier sous l'angle du management des risques. Cette lacune a rendu l'établissement d'une compréhension exhaustive des bases théoriques et des retours d'expérience formalisés plus complexes.

- **Contraintes d'échantillonnage et de représentativité des entretiens :**

En raison de contraintes d'agendas, d'annulations imprévues et des difficultés d'accès prolongé à certains professionnels clés, le nombre d'entretiens réalisés a été plus limité que ce qui était initialement envisagé. Bien que ces échanges aient apporté une richesse d'informations qualitative précieuse et des perspectives éclairantes, ils réduisent inévitablement la représentativité et la diversité des retours d'expérience. L'étude n'a pu couvrir qu'un éventail restreint de typologies d'établissements et de contextes géographiques (notamment les spécificités des territoires ruraux ou ultra-marins).

- **Nature déclarative des données recueillies et sensibilité des informations :**

Les informations collectées reposent principalement sur le discours des professionnels interrogés. Cette nature déclarative présente des limites inhérentes, telles que la possible minimisation de certaines difficultés, la réticence naturelle à partager des failles internes ou des détails d'incidents, ou une perception parfois optimiste des pratiques réelles due à la nature sensible des données de cybersécurité. L'accès direct à des données d'observation ou à des documents internes détaillés n'a pas été possible, ce qui peut influencer l'objectivité de certains constats et rendre l'analyse plus conceptuelle

qu'empirique, limitant la profondeur des illustrations pratiques.

c) La portée thématique ciblée au regard de la transversalité croissante de la cybersécurité

Enfin, une limite de cette étude réside dans sa portée thématique volontairement ciblée sur les aspects managériaux, organisationnels et pratiques de la cybersécurité en lien avec le management des risques, de la qualité et des flux, et ce, spécifiquement pour le secteur de la santé. Cette approche a permis d'approfondir des aspects clés, mais elle ne peut embrasser l'intégralité des ramifications de la cybersécurité.

En effet, si cette dernière fut longtemps perçue comme un problème purement technique relevant de la seule direction des systèmes d'information, l'analyse actuelle révèle son caractère éminemment transversal. Elle touche désormais absolument tous les domaines de l'entreprise, des processus métiers à la gestion des ressources humaines, en passant par la chaîne d'approvisionnement et même les questions éthiques ou juridiques complexes. Cette prise de conscience, relativement récente, transforme progressivement l'organisation des entreprises. Par conséquent, ce mémoire n'a pas abordé en profondeur des dimensions importantes telles que les impacts humains profonds (stress professionnel, réactions psychologiques face aux crises cyber), les questions éthiques complexes (confidentialité et intégrité des données patient, droit à l'information en cas de fuite), ou les aspects juridiques détaillés, qui sont pourtant essentiels dans le secteur hospitalier.

4.2. Pistes de recherche futures

Les limites identifiées dans cette étude, conjuguées à la constante évolution du paysage de la cybersécurité en santé, ouvrent de nombreuses et prometteuses voies pour de futures recherches. Celles-ci pourraient enrichir notre compréhension de la cyber-résilience hospitalière sous l'angle du management en santé et contribuer à renforcer la sécurité des parcours de soins.

a) Évaluation approfondie de l'impact des programmes et méthodes

- **Études quantitatives de l'efficacité et du retour sur investissement :** une perspective essentielle consisterait à réaliser des études à plus grande échelle pour

quantifier précisément l'impact du programme CaRE sur la réduction effective des incidents de cybersécurité, ou sur l'amélioration mesurable de la maturité cyber des établissements. Cela permettrait également d'évaluer le retour sur investissement des mesures de cybersécurité mises en place, en traduisant ces investissements en termes concrets de continuité des soins, de sécurité des patients et de protection des données.

- **Analyse comparative et longitudinale des implémentations d'EBIOS RM et CaRE :** il serait pertinent de mener une analyse comparative de l'adoption, des défis rencontrés et des bénéfices réels de ces deux cadres (CaRE et EBIOS RM) au sein de différentes typologies d'établissements de santé (CHU, Centres Hospitaliers, hôpitaux locaux, cliniques privées). Une telle étude devrait prendre en compte leurs ressources spécifiques, leur taille et leurs particularités organisationnelles. Une approche longitudinale, suivant l'évolution de l'appropriation et des résultats sur plusieurs années, serait particulièrement éclairante pour comprendre les dynamiques à long terme.

b) Renforcement de la compréhension des pratiques opérationnelles

- **Observation directe et études de cas approfondies :** Pour compléter les données déclaratives, souvent soumises aux biais et aux réticences liées à la sensibilité du sujet, de futures recherches pourraient privilégier des approches qualitatives basées sur l'observation directe des pratiques. Cela inclurait par exemple l'observation participante lors d'exercices de gestion de crise simulés, la participation à des audits internes de cybersécurité, ou, avec les consentements nécessaires et l'anonymisation des données, le suivi détaillé de cas réels d'incidents cyber. Ces méthodes permettraient de saisir la complexité des dynamiques en temps réel et de confronter les discours aux actions concrètes.
- **Cybersécurité pour tous les territoires et la force du partage :** Il serait utile de mieux comprendre comment les établissements de santé s'organisent face aux cyberattaques, en particulier ceux situés dans des zones plus isolées (comme les zones rurales ou les Outre-mer), qui peuvent manquer de ressources spécialisées. Il serait aussi intéressant d'étudier comment le partage des compétences et des équipements entre hôpitaux (par exemple, en créant des "centres de surveillance" communs pour plusieurs établissements, appelés SOC mutualisés au sein des GHT) peut aider l'ensemble du système de santé à mieux résister aux attaques.

L'objectif est de voir comment la collaboration renforce la sécurité de tous.

c) Exploration des dimensions émergentes de la cybersécurité en santé

- **L'intégration de la cybersécurité dans la formation initiale et continue des professionnels de santé :** Au-delà des sensibilisations ponctuelles, il est crucial d'étudier comment intégrer de manière systématique et approfondie la cybersécurité dans la formation initiale des futurs médecins, infirmiers, managers, et autres professionnels de santé. Cela inclut également la formation continue, pour maintenir les compétences à jour face à l'évolution rapide des menaces. Comment concevoir des cursus pertinents et adaptés aux différents profils ? Quels sont les modèles pédagogiques les plus efficaces ? Comment évaluer l'impact de ces formations sur les pratiques réelles ?
- **Les impacts humains, éthiques et juridiques des cyber-crises :** Notre étude a effleuré la transversalité de la cybersécurité ; des recherches spécifiques pourraient être développées sur les aspects humains des cyber-crises (gestion du stress, résilience psychologique des équipes, impact sur la satisfaction au travail) et les dilemmes éthiques et juridiques complexes rencontrés par les établissements face à la compromission des données de santé, l'interruption des soins ou la rançon. Cela inclurait l'analyse des cadres légaux et réglementaires en constante évolution (ex : NIS2) et leur application pratique [49].
- **L'impact des technologies innovantes sur la sécurité :** Les avancées technologiques comme l'intelligence artificielle (IA), qui aide par exemple au diagnostic, ou les objets connectés médicaux (comme les capteurs pour patients, les pompes à insuline intelligentes), apportent des améliorations significatives aux soins. Cependant, ces nouvelles technologies introduisent également de nouvelles failles de sécurité potentielles. Il devient essentiel d'étudier comment protéger ces outils innovants et les données qu'ils génèrent, pour garantir qu'ils restent un atout pour les patients et les soignants, sans devenir une porte d'entrée pour les cyberattaques. Cette recherche permettrait d'anticiper les défis de demain.

Ces pistes de recherche futures témoignent de la richesse et de la complexité persistante de la cybersécurité en santé. Ce domaine est en mutation rapide, où les avancées technologiques et organisationnelles doivent impérativement s'aligner sur les exigences éthiques et humaines fondamentales de la mission de soin, et où la recherche peut jouer un rôle déterminant dans l'amélioration continue de la résilience du système de santé.

CONCLUSION GÉNÉRALE

La cybersécurité dans les établissements de santé ne représente plus seulement un enjeu technique, mais bien un impératif stratégique et humain. Ce mémoire a montré qu'en dépit des initiatives actuelles, telles que le programme CaRE et la méthode EBIOS RM, les établissements demeurent fragiles face aux cyberattaques de plus en plus sophistiquées.

Le programme CaRE offre une réponse claire et opérationnelle essentielle pour gérer efficacement une crise cyber. Cependant, sa pleine efficacité nécessite encore un véritable changement culturel et organisationnel. La sensibilisation et la formation du personnel restent critiques, car c'est souvent l'humain qui constitue la première ligne de défense face aux attaques numériques.

Par ailleurs, la méthode EBIOS RM propose une approche anticipative indispensable, complémentaire à CaRE, permettant aux établissements d'identifier proactivement les risques et de prioriser les mesures de sécurité adaptées aux spécificités hospitalières. Son adoption effective exige toutefois un accompagnement plus réaliste et accessible, particulièrement pour les structures aux ressources limitées.

Pour renforcer durablement la résilience des établissements de santé, il est impératif d'intégrer étroitement anticipation et réaction. Les décideurs doivent désormais adopter une logique de gestion des crises systémiques, dépassant les silos techniques, organisationnels et humains. Ainsi, en conjuguant anticipation stratégique et réponse opérationnelle, les établissements pourront réellement protéger leurs patients, leurs données sensibles et leur mission première : prodiguer des soins continus et sécurisés.

Bibliographie

[1] Le Figaro. (2022). Dans l'hôpital de Corbeil-Essonnes, visé par une cyberattaque, couloirs déserts et familles inquiètes. Article de presse en ligne] Disponible sur : https://www.lefigaro.fr/dans-l-hopital-de-corbeil-essonnes-vise-par-une-cyberattaque-couloirs-deserts-et-familles-inquietes-20220823

[2] PwC France 2022. Les défis de la cybersécurité dans les établissements de santé en France, *PricewaterhouseCoopers France*, 42 p.

[3] FARIHA T., ALENEZI M., & ALMAJED A., 2021. Cybersecurity in Medical IoT: Threats and Defense Strategies, *Computer Communications*, 173, p. 139–154.

[4] ENISA. (2016). Cyber security and resilience for Smart Hospitals. [Rapport en ligne]. Disponible sur : https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Hospitals.pdf

[5] IBM SECURITY, (2022). Cost of a Data Breach Report. IBM Security & Ponemon Institute, 78 p. [Rapport en ligne] Disponible sur : https://www.ibm.com/reports/data-breach

[6] DUFOUR J., MARTIN A. & LEGRAND C., (2023). Gestion des crises cyber en milieu hospitalier. Revue Santé Numérique, 7(2), p. 21–35. [Article de journal]

[7] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). (2025). Plan stratégique 2025-2027 : Au cœur d'un collectif, pour une Nation cyber-résiliente. (Consulter les sections d'introduction et les axes stratégiques sur la résilience et la gestion de crise. [Plan stratégique] disponibles sur : https://cyber.gouv.fr/sites/default/files/document/Plan-strat%C3%A9gique-2025-2027-de-lANSSI.pdf

[8] ANSSI, (2021). Guide d'hygiène informatique pour les établissements de santé. [Guide en ligne] Disponible sur : https://cyber.gouv.fr/publications/guide-dhygiene-informatique

[9] Cert santé, (2023). Panorama de la cybercriminalité. [Rapport en ligne] Disponible sur : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf

[10] ANSSI, (2021). Guide crise d'origine cyber. [Guide en ligne] Disponible sur :https://cyber.gouv.fr/sites/default/files/2021/12/anssi-guide-gestion_crise_cyber.pdf

[11] ISO 31000 : 2018. Management du risque - Lignes directrices. [Norme en ligne] Disponible sur : https://www.iso.org/obp/ui/fr/#iso:std:iso:31000:ed-2:v1:fr

[12] AFNOR, (2020). La cybersécurité appliquée au secteur de la santé, Guide pratique. Association Française de Normalisation, Paris. [Guide pratique]

[13] Lagadec, P. (2012) – La gestion des crises : outils de gestion de crise pour décideurs, Dunod. [Livre]

[14] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), (2023). Panorama des menaces informatiques 2022-2023. [Rapport en ligne] Disponible sur : https://cyber.gouv.fr/actualites/lanssi-publie-le-panorama-de-la-cybermenace-2023

[15] ENISA. [Rapports] disponible sur : https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[16] Agence du Numérique en Santé (ANS). (2023). Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social 2023. [Rapport en ligne] disponible sur : https://esante.gouv.fr/sites/default/files/media_entity/documents/observatoire-incidents-cybersecurite-sante-2023.pdf

[17] ANSSI, (2022). Rapport annuel sur la cybersécurité en France. Agence Nationale de la Sécurité des Systèmes d'Information, 88 p. [Rapport en ligne] disponible sur : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

[18] IBM Security & Ponemon Institute. (2024). Cost of a Data Breach Report 2024. [Rapport en ligne] disponible sur :

https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

[19] Le Monde, (2019). Une cyberattaque perturbe les soins au CHU de Rouen. [Article de presse en ligne] Disponible sur : https://www.lemonde.fr/sante/article/2019/11/17/

[20] ZATAZ. (14 février 2021). Plus de 400.000 données de patients français vendus dans le blackmarket. [Article en ligne] disponible sur : https://www.zataz.com/plus-de-400-000-donnees-de-patients-francais-vendus-dans-le-blackmarket/

[21] Comité Consultatif National d'Éthique (CCNE), (2022). Avis n°130 : données massives et santé : une nouvelle approche des enjeux éthiques. [Avis en ligne] Disponible sur : https://www.ccne-ethique.fr/sites/default/files/2021-02/avis_130.pdf

[22] Règlement général sur la protection des données (RGPD), (2016). [Règlement en ligne] Disponible sur : https://eur-lex.europa.eu/eli/reg/2016/679

[23] Commission Nationale de l'Informatique et des Libertés (CNIL), (2022). Rapport annuel commission nationale de l'informatique et des libertés. [Rapport en ligne] Disponible sur : https://www.cnil.fr/sites/cnil/files/2023-05/cnil_-_43e_rapport_annuel_-_2022.pdf

[24] Loi de Programmation Militaire (LPM), (2019-2025). Obligations des opérateurs de services essentiels en cybersécurité. [Texte de loi en ligne] Disponible sur : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037192797?page=1&pageSize=10&query=loi+de+programmation+militaire

[25] ISO/IEC, (2022). ISO/IEC 27005 – Information security risk management – aligné avec la méthode EBIOS. [Norme en ligne] Disponible sur : https://www.iso.org

[26] Association Française de Normalisation (AFNOR), (2020). Guide pratique ISO 27001 appliqués au secteur hospitalier. AFNOR Éditions, Paris. [Guide pratique]

[27] Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel. [Texte de loi en ligne] Disponible sur : https://www.legifrance.gouv.fr

[28] Agence du Numérique en Santé (ANS), (2022). Référentiel Hébergeur de Données de Santé (HDS). [Référentiel en ligne] Disponible sur https://esante.gouv.fr/actualites/le-referentiel-de-certification-applicable-aux-hebergeurs-de-donnees-de-sante-hds-evolue

[29] Ministère de la Santé et de la Prévention, (2023). Programme Cybersécurité Accélération et Résilience des Établissements (CaRE). [Programme en ligne] Disponible sur :https://sante.gouv.fr/actualites/presse/communiques-de-presse/article/presentation-du-plan-care-proteger-les-etablissements-de-sante-face-a-la-menace

[30] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), (2018). Méthode EBIOS Risk Manager - Guide méthodologique. [Guide en ligne] Disponible sur : https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide

[31] ALL4TEC, (2025). Entretien expert cyber, 7 avril 2025 – méthode EBIOS RM et analyse de risque cyber en santé. [Entretien]

[32] Entretien technicienne informatique, 5 mai 2025,

[33] Agence du Numérique en Santé (ANS), (2023). Présentation du programme CaRE. [Présentation en ligne] Disponible sur : https://esante.gouv.fr/espace-presse/presentation-du-programme-care

[34] Ministère de la Santé et de la Prévention, (2019). Feuille de route “Accélérer le virage numérique” - dossier d'information. [Dossier en ligne] Disponible sur https://sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf

[35] Le Monde, (2021). L’hôpital de Dax en partie paralysé par une attaque informatique. [Article de presse en ligne] Disponible sur : https://www.lemonde.fr

[36] HOUTAIN S., (2022). Cybersécurité : ne vaut-il pas mieux prévenir que guérir ? Risques et Qualité en Milieu de Soins, p. 12-16a et p. 17-22b. [Article de revue en ligne] Disponible sur https://stm.cairn.info/revue-risques-et-qualite-en-milieu-de-soins-2022-1-page-12?lang=fr

[37] Agence du Numérique en Santé (ANS), (2023). Le plan d’action pour protéger nos établissements face à la menace cyber. [Plan d'action en ligne] Disponible sur https://esante.gouv.fr/sites/default/files/media_entity/documents/doc-programme-care-231214-20h_pap%5B17%5D.pdf

[38] Ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique, (octobre 2024). France 2030 : stratégie d'accélération santé numérique. [Stratégie en ligne] Disponible sur https://www.entreprises.gouv.fr/priorites-et-actions/autonomie-strategique/soutenir-linnovation-dans-les-secteurs-strategiques-10

[39] Cour des Comptes, (2019). Observations définitives : la sécurité informatique des établissements de santé, p. 50. [Rapport en ligne] Disponible sur : https://www.ccomptes.fr/sites/La-securite-informatique-des-etablissements-de-sante.pdf

[40] Agence du Numérique en Santé, (2024). Support Atelier Cyber PCRA SantExpo 2024. [Présentation en ligne] Disponible sur https://esante.gouv.fr/sites/default/files/media_entity/documents/santexpo-2024---atelier-pcra.pdf

[41] Weliom & ALL4TEC, (14 décembre 2023). La méthode EBIOS RM modélisée pour les établissements de santé. [Webinaire en ligne] Disponible sur

https://www.all4tec.com/blog/webinaires/la-methode-ebios-rm-modelisee-pour-les-etablissements-de-sante/

[42] ALL4TEC, (juin 2024). Conférence Analyse de risques cyber - EBIOS RM à l'épreuve de l'hôpital et de ses partenaires. [Conférence en ligne] Disponible sur : https://www.youtube.com/watch?v=AbDI3j5A29k

[43] ANS webinaire Programme CaRE - Présentation des kits d'exercice de crise V2 ; [Webinaire] disponible sur : https://www.youtube.com/watch?v=exercice_de_crise_V2

[44] webinaire - Renforcer votre cyber résilience avec le Domaine 2 du programme CaRE" (Orange Cyberdéfense, 29 avril 2025).

[45] ANS webinaire Programme CaRE Atteinte des objectifs Domaine 1 - Questions fréquentes et points d'attention, (11 avril 2025) disponible sur : https://youtu.be/aiYJkj7odWw?si=63AFT2kLFHfa08WC

[46] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), (2024). Secteur de la santé : état de la menace informatique. [Rapport en ligne] Disponible sur : https://cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-010.pdf

[47] Schneier, B. (2023, 23 mars). Why Take9 Won't Improve Cybersecurity. Schneier on Security. [Blog] disponible sur : https://www.schneier.com/blog/archives/2025/05/why-take9-wont-improve-cybersecurity.html

[48] Schneier, B. (2016). Stop Trying to Fix the User. IEEE Security & Privacy, 14(5), 8-12. [Article] disponible sur: https://www.schneier.com/wp-content/uploads/2016/09/Stop-Trying-to-Fix-the-User-IEEE-SP.pdf

[49] Directive (UE) 2022/2555 du parlement européen et du conseil du 14 décembre 2022. Concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'union. [Directive en ligne] Disponible sur. https://eur-lex.europa.eu/La directive NIS 2

Table des matières

Remerciements 2
Sommaire 3
Introduction 5
PARTIE I : CYBERSÉCURITÉ EN SANTÉ : DE LA GESTION DES RISQUES À LA GESTION DE CRISE 8
1. Définitions 8
a) Cybersécurité, cyber risque et crise cyber 8
b) La gestion des risques et la gestion de crise 9
2. Typologie et impacts des cyberattaques en santé 9
a) Les vecteurs d'attaque courants 9
b) Les charges utiles et leurs conséquences 10
c) L'ampleur de la menace et ses coûts 11
d) Une réalité critique 12
3. Enjeux spécifiques au secteur hospitalier 13
a) Enjeu sur la continuité des soins 13
b) Enjeu sur la confidentialité des données 13
c) Enjeu sur l'éthique 14
4. Cadre réglementaire et politique publique 14
a) Réglementation européenne 14
b) Réglementation nationale 15
c) Les normes 15
PARTIE II : ANTICIPER POUR MIEUX GÉRER : LES OUTILS STRATÉGIQUES EN AMONT DE LA CRISE 18
1. Présentation de la méthode EBIOS Risk Manager 18
2. Application potentielle ou réelle dans les établissements de santé 20
a) Illustrations pratiques de la complémentarité EBIOS RM et CaRE : Retours d'expérience des professionnels de santé 21
b) Des opportunités mais des freins culturels à dépasser 24
3. Limites de l'approche purement anticipative face aux cyberattaques actuelles 24
3.1. Une réalité cyber mouvante et incertaine 24
3.2. Des attaques innovantes et difficilement modélisables 25
3.3. Une gestion des risques encore trop statique et cloisonnée 26
3.5. Le besoin d'un écosystème intégré : anticiper et réagir 26
a) Anticiper, oui, mais sans illusion d'exhaustivité 26
PARTIE III : LE PROGRAMME CYBERSÉCURITÉ ACCÉLÉRATION, RÉSILIENCE DES ÉTABLISSEMENTS : RÉPONSES AUX CRISES CYBER EN MILIEU HOSPITALIER 28
1. Genèse, objectifs et structure du programme CaRE 28
1.1. Une réponse à un déficit structurel de préparation 28
1.2. Objectifs stratégiques du programme CaRE 29
1.3. Structuration et financement du programme 29
a) Une réponse bienvenue, mais tardive et perfectible 30
2. Dispositifs et actions en cas de cybercrise 30
2.1. Domaine 1 : audits techniques et remédiation des vulnérabilités 30

2.2. Domaine 2 : continuité et reprise d'activité (CRA)....31
2.3. Soutiens externes, partenariats et mutualisation.... 32
2.4. Un pas décisif, mais pas encore structurant....32
3. Forces et faiblesses de CaRE dans sa mise en œuvre concrète.... 32
a) Une prise de conscience à tous les niveaux....33
b) Le kit PCRA, un outil pragmatique et accessible....33
c) L'effet pédagogique des audits.... 33
4. Analyse comparative des forces de CaRE et des axes d'amélioration inspirés d'EBIOS...34
4.1. Les points forts de CaRE....34
4.2. Les limites de CaRE....35
4.3. Ce qu'EBIOS RM peut apporter.... 35
4.3. Une synergie à construire au service de la résilience réelle.... 36
PARTIE IV : TERRAIN ET RETOURS D'EXPÉRIENCE....37
1. Méthodologie de l'étude qualitative....37
a) Positionnement épistémologique....37
1. 1. Méthodologie de collecte des données....37
a) Des entretiens semi-directifs 37
b) Analyse de webinaires de retours d'expérience.... 38
c) Échantillonnage.... 38
d) Analyse des données.... 39
e) Limites de la méthodologie....39
1.2. Présentation des participants et des contextes....40
1) RSSI.... 40
2) Expert Cyber & RSSI de ALL4TEC.... 40
3) Coordonnateur Situation Sanitaire Exceptionnelle (SSE)....41
4) Responsable du Système d'Information (RSI)....41
5) Technicienne informatique....41
2. État des lieux de la gestion des cyber-risques dans les établissements de santé.... 42
2.1. Conscience de la menace et fréquence des incidents....42
2.2. Mesures techniques de prévention et de détection existantes....43
2.3. Utilisation et perception des outils et méthodes de gestion des risques (hors EBIOS et CaRE)..... 44
3. Le programme CaRE à l'épreuve du terrain : Analyse de son impact sur la gestion des crises cyber.... 45
3.1. Déploiement et appropriation du programme CaRE.... 45
3.2. Apports concrets de CaRE pour la gestion des crises cyber.... 46
a) Structuration de la réponse à crise....46
b) Montée en compétence collective.... 46
c) Renforcement des stratégies de continuité et de reprise d'activité (PCA/PRA).... 46
d) Protection des systèmes et des données....47
e) Témoignage sur la capacité à réagir et à se coordonner.... 47
3.3. Défis et limites du programme CaRE....47
a) Contraintes de ressources (humaines, financières) pour le déploiement....47
b) Difficultés d'intégration avec les processus existants....48
c) Besoins d'adaptation à la taille et aux spécificités de chaque établissement.... 48
d) La question de la pérennisation des efforts au-delà des exercices....48

4. La méthode EBIOS : levier pour renforcer la résilience..... 48
4.1. Connaissance et adoption d'EBIOS RM dans le secteur de la santé.....49
4.2. Contributions d'EBIOS à la compréhension et à la maîtrise des risques..... 49
a) Identification et analyse approfondie des menaces et vulnérabilités.....49
b) Définition de scénarios de risque.....50
c) Évaluation de la couverture des mesures de sécurité existantes..... 50
d) Aide à la décision et à la priorisation des investissements de sécurité..... 50
4.3. Défis et opportunités d'EBIOS pour les établissements de santé..... 51
a) Complexité perçue de la méthode et besoin d'expertise..... 51
b) Intégration des résultats d'EBIOS dans les plans d'action opérationnels.....51
c) Retour d'expérience sur l'adaptation d'EBIOS au contexte hospitalier.....51
d) EBIOS comme outil de sensibilisation interne et de dialogue avec la direction..... 52
5. Synergie et complémentarité perçues entre EBIOS et CaRE..... 52
5.1. Comment l'approche par les risques d'EBIOS affine la préparation CaRE.....52
5.2. La perception d'une complémentarité entre l'analyse et l'entraînement.....53
5.3. Facteur facilitant ou freinant cette synergie sur le terrain.....53
a) Facteurs facilitants.....53
b) Facteurs freinant.....53
PARTIE V : PRÉCONISATIONS STRATÉGIQUES POUR UNE CYBERSÉCURITÉ INTÉGRÉE.. 55
1. Des cadres nationaux à la résilience..... 55
a) Complémentarité pour une approche globale des risques..... 55
b) L'intégration des risques cyber dans le management de la qualité des soins.....56
c) Un cadre national structurant au service de la performance organisationnelle..... 56
d) L'humain et l'organisation au cœur de la résilience.....57
2. Recommandations concrètes pour les établissements.....57
2.1. Recommandations managériales : faire de la cybersécurité une priorité stratégique et transversale... 57
2.2. Recommandations opérationnelles.....58
a) Gestion des Actifs et Analyse des Risques..... 58
b) Renforcement de la Continuité et de la Résilience Opérationnelle..... 59
c) Mesures Techniques et Organisationnelles Fondamentales..... 59
2.3. Recommandations en formation et sensibilisation..... 60
a) La cybersécurité en santé : Priorité aux systèmes, pas seulement aux utilisateurs.....60
b) Doter l'Ensemble du Personnel des Réflexes de Base..... 60
c) Sensibilisation Ciblée des Cadres et Implication des Équipes..... 60
d) Simplification de la Communication et Formations Croisées.....61
e) Conclusion des recommandations.....61
3. Perspectives : vers une culture de la cybersécurité en santé..... 62
4. Limites de l'étude et pistes de recherche futures.....63
4.1. Limites de la présente étude..... 63
a) Le caractère récent des cadres et outils étudiés et le manque de recul opérationnel.....63
b) Les contraintes liées à la collecte de données empiriques.....64
c) La portée thématique ciblée au regard de la transversalité croissante de la cybersécurité..... 65
4.2. Pistes de recherche futures.....65

a) Évaluation approfondie de l'impact des programmes et méthodes..... 65
b) Renforcement de la compréhension des pratiques opérationnelles..... 66
c) Exploration des dimensions émergentes de la cybersécurité en santé..... 66
CONCLUSION GÉNÉRALE..... 68
BIBLIOGRAPHIE..... 69
ABRÉVIATIONS..... 79
Annexes..... 1

Abréviations

AFNOR : Association Française de Normalisation

ANS : Agence du Numérique en Santé

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

ARS : Agence Régionale de Santé

BIA : Bilan d'Impact sur l'Activité

CCNE : Comité Consultatif National d'Éthique

CERT : Computer Emergency Response Team

CH : Centre Hospitalier

CHSF : Centre Hospitalier Sud Francilien

CHU : Centre Hospitalier Universitaire

CLUSIF : Club de la Sécurité de l'Information Français

CME : Commission Médicale d'Établissement

CNIL : Commission Nationale de l'Informatique et des Libertés

CRA : Continuité et Reprise d'Activité

CSIRMT : Commission des Soins Infirmiers, de Rééducation et Médico-Techniques

DSI : Direction des Systèmes d'Information

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ENISA : European Union Agency for Cybersecurity

GHT : Groupement Hospitalier de Territoire

HDS : Hébergeur de Données de Santé

IBM : International Business Machines

IEC : International Electrotechnical Commission

ISO : Organisation Internationale de Normalisation

IT : Information Technology (Technologies de l'Information)

LPM : Loi de Programmation Militaire

OSE : Opérateur de Services Essentiels

PCA : Plan de Continuité d'Activité

PCRA : Plan de Continuité et de Reprise d'Activité

PSSI : Politique de Sécurité des Systèmes d'Information

RETEX : Retour d'Expérience

RGPD : Règlement Général sur la Protection des Données

RM : Risk Manager

RPCRA : Référent Plan de Continuité et Reprise d'Activité

RSI : Responsable des Systèmes d'Information

RSMCA : Référentiel de Sécurité des Moyens de Communication d'Alerte

RSSI : Responsable de la Sécurité des Systèmes d'Information

SCA : Système Critique d'Activité

SI : Système d'Information

SOC : Security Operations Center

SRA : Système de Reprise d'Activité

SSE : Situation Sanitaire Exceptionnelle

UE : Union Européenne

Annexes

Annexe 1 : Guide d'entretien 2

Annexe 2 : Entretien avec une technicienne informatique 4

Annexe 3 : entretien avec l'expert cyber & RSSI 8

Annexe 1 : Guide d'entretien

Date de l'entretien :

Lieu de l'entretien :

Durée de l'entretien :

Dans quelle mesure le programme Cybersécurité accélération et Résilience des Établissements (CaRE) permet-il aux établissements de santé de gérer les crises liées aux cyberattaques et quels enseignements tirer de la méthode EBIOS pour renforcer cette résilience ?

I. Renseignements personnels

---

1. Pouvez-vous vous présenter et expliquer votre rôle dans l'établissement ? (Identité, fonction, établissement, expérience sur la gestion des risques cyber).
2. Avez-vous déjà été confronté à une cyberattaque dans votre établissement ?

II. Contexte sur la gestion des risques

---

1. Comment votre établissement anticipe-t-il les cyber-risques aujourd'hui ?
2. Utilisez-vous une méthode ou un outil formalisé pour évaluer ces risques (ex. : cartographie, analyse de criticité) ?
3. Connaissez-vous la méthode EBIOS ? L'utilisez-vous ou vous en inspirez-vous ? Pourquoi (ou pourquoi pas) ?

III. Mise en œuvre et efficacité du programme CaRE

---

1. Êtes-vous familier avec le programme CaRE ? Si oui, comment est-il appliqué chez vous ?
2. Selon vous, CaRE est-il efficace pour répondre à une crise cyber ? Quels sont ses principaux apports ?
3. Quelles difficultés ou limites rencontrez-vous avec ce programme ?
4. En cas d'attaque, existe-t-il un plan de gestion de crise dans votre établissement ? Est-il efficace selon vous ?

IV. Comparaison avec la méthode EBIOS

1. Pensez-vous que des éléments d'EBIOS pourraient compléter ou renforcer CaRE ?
2. Comment pourriez-vous combiner préparation (risques) et réaction (crise) de manière plus efficace ?

V. Retours d'expérience

1. Si vous deviez partager un enseignement clé de votre expérience avec CaRE ou EBIOS, quel serait-il ?
2. Quels conseils donneriez-vous à un établissement souhaitant adopter ces outils ?

VI. Suggestions et perspectives

1. Quel est, selon vous, le principal enseignement à retenir d'un incident cyber vécu ou anticipé ?
2. Que recommanderiez-vous à un établissement pour mieux se préparer aux cyberattaques ?
3. Selon vous, quelles améliorations seraient nécessaires dans les approches actuelles ?

VII. Conclusion

1. Y a-t-il un point important que vous souhaitez ajouter ?
2. Seriez-vous d'accord pour être recontacté si besoin de précision ?

Annexe 2 : Entretien avec une technicienne informatique

Présentation

[00:00:00 – 00:02:15]

Bonjour et merci beaucoup pour ce temps ! Pour commencer, je suis curieuse de savoir comment vous vous présentez dans votre rôle au quotidien.

Technicienne SI : Bonjour ! Oui, bien sûr. Je suis technicienne au service informatique, et je fais partie de l'équipe qui gère l'ensemble du système d'information de l'établissement. Ça va de la gestion des postes et des serveurs à la sécurité des accès et des données. Je suis là depuis six ans, et ça fait un peu plus de deux ans que je suis impliquée directement dans les questions de cybersécurité, notamment pour la mise en place du programme CaRE et des exercices de gestion de crise.

Et du coup, vous avez déjà eu à gérer une crise cyber pour de vrai ?

Technicienne SI : Oui, on a eu un incident sérieux il y a trois ans : un phishing bien ficelé qui avait failli passer, mais heureusement on a réagi à temps. Depuis, on est beaucoup plus vigilants, et surtout on a compris que la gestion de crise ne se limite pas à la technique.

Comment ça se traduit au quotidien, la préparation aux cyber-risques ?

Technicienne SI : C'est un peu un réflexe maintenant ! On fait de la veille tous les jours sur les failles et les alertes, et on met à jour nos cartographies et nos analyses de risques régulièrement. On essaie aussi de sensibiliser le personnel avec des petites fiches pratiques et des formations, parce que c'est souvent là que ça pêche : l'humain est la première ligne de défense.

Gestion des risques : Échange autour d'EBIOS

Utilisez-vous un outil ou une méthode formalisée pour évaluer les risques, comme de la cartographie ou une analyse de criticité ?

Technicienne SI : Oui, pour la cartographie, on a un outil qui nous permet de voir en temps réel les postes, les serveurs, les interconnexions. Et pour l'analyse de criticité, on utilise un tableau de bord avec des critères définis : confidentialité, intégrité, disponibilité… ça nous aide à prioriser les actions.

Vous connaissez la méthode EBIOS ? Est-ce que vous l'utilisez ou vous vous en inspirez ? Pourquoi ou pourquoi pas ?

Technicienne SI : Oui ! On l'a découvert par notre RSSI qui nous l'a présenté en réunion. Et ça a été un vrai déclencheur : avant, on faisait surtout des audits techniques, mais EBIOS nous a aidés à structurer la réflexion plus globalement. Aujourd'hui, on ne l'applique pas à la lettre, parce qu'il y a des parties très lourdes, mais on s'en inspire beaucoup. Ce qui nous plaît dans EBIOS, c'est qu'elle oblige à se poser les bonnes questions : qui pourrait nous attaquer ? Pourquoi ? Avec quels moyens ?

Concrètement, comment vous l'avez intégré dans vos pratiques ?

Technicienne SI : On a commencé par reprendre les grands principes : les événements redoutés, les scénarios de menace, les mesures existantes… Ça a été une grosse étape pour nous, parce que ça oblige à se mettre à la place de l'attaquant, à réfléchir à ses motivations et à ses moyens. On a fait des ateliers internes pour essayer de voir les points faibles de nos systèmes : par exemple, les accès partagés dans certains services ou les mots de passe qui traînent sur des post-its. EBIOS nous a permis de prioriser les risques, pas seulement de lister les failles.

Est-ce que ça a changé la façon dont vous voyez la sécurité ?

Technicienne SI : Carrément ! Avant, c'était « on corrige les vulnérabilités techniques » et ça s'arrêtait là. Maintenant, on regarde l'ensemble de l'écosystème : les utilisateurs, les prestataires, les données sensibles… Et surtout, ça nous donne un vocabulaire commun pour échanger avec la direction, parce que ce n'est pas toujours simple de leur faire vous parlez de limites ou de difficultés à l'adopter ?

Technicienne SI : Au début, ça nous a paru trop théorique. On s'est dit « OK, c'est bien beau, mais comment on l'applique ? ». Il a fallu faire des formations internes, des tests, et surtout beaucoup de simplification. Le jargon peut perdre les non-initiés ! On a dû trouver un équilibre entre le cadre d'EBIOS et nos réalités terrain.

Et aujourd'hui, diriez-vous que ça vous aide toujours ?

Technicienne SI : Oui, on s'en sert toujours, surtout en amont des exercices ou des mises à jour de nos procédures. Par exemple, quand on prépare un nouveau scénario de crise, on part toujours des scénarios d'attaque d'EBIOS : ça nous donne un socle très solide. Après, on adapte pour que ce soit opérationnel.

[00:15:47 - 00:48:03]

Gestion de crise et programme CaRE

Merci pour ces précisions. J'aimerais qu'on parle du plan de cyber sécurité, accélération et résilience des établissements ou tout simplement care. J'ai cru comprendre que vous avez déployé CaRE et atteint les objectifs du domaine 1 ?

Technicienne SI : Oui, on l'a déployé il y a un an et demi. Ça a été un gros chantier parce que ça touche toute la gouvernance cyber. Le domaine 1, c'est beaucoup de documentation : politiques de sécurité, processus de validation, définition des rôles et responsabilités. Ça nous a obligés à tout clarifier.

Lors de mes recherches documentaires, j'ai vu que l'un des critères du domaine 1 et la réalisation d'exercice de crise, vous en avez fait chez vous ou pas ?

Technicienne SI : Exactement ! On a fait deux exercices de simulation de crise pour tester la réactivité de nos équipes. Le premier, c'était un scénario interne avec un phishing massif : l'idée était de voir comment les équipes réagissaient. Le deuxième, plus complet, on l'a fait en décembre en faisant intervenir un prestataire externe pour simuler un ransomware où un agent avait inséré un objet infecté par erreur. Je vous partage le rapport de l'exercice.

Merci pour ce partage. Il a l'air très réaliste !

Technicienne SI : Oui, on a vraiment cherché à coller au maximum à ce qui pourrait nous arriver. C'était stressant, mais tellement formateur ! On a vu qu'au-delà de la technique, c'est l'organisation et la communication qui font toute la différence. Ça a montré qu'on avait encore des progrès à faire, surtout sur la communication en cas de crise.

Qu'est-ce qui vous a marquée pendant cet exercice ?

Technicienne SI : Plusieurs choses ! D'abord, la montée en puissance progressive du scénario : au début, c'était juste un petit incident, puis ça s'est aggravé jusqu'au blocage complet des services. Ça a mis tout le monde sous pression, et on a vu que nos fiches réflexes n'étaient pas encore assez connues. On a aussi compris qu'on devait absolument préparer les canaux de communication internes : qui dit quoi, à qui, et comment on rassure les équipes.

Et le rapport de l'exercice, vous l'avez bien exploité ensuite ?

Technicienne SI : Ah oui, nous l'avons décortiqué en réunion de crise. Les points positifs, c'est qu'on a une bonne réactivité et un bon réflexe d'appeler directement l'équipe SSI du groupe : pas de panique, pas de déconnexion sauvage ! Les points d'amélioration, c'était surtout la traçabilité : par exemple, chaque partie prenante, noté ce qu'il a fait pendant cette période, pas dans les détails, il y 'a eu des oublis forcément. On a aussi travaillé depuis sur la rédaction de mails-types pour les communications de crise, parce que dans le feu de l'action, c'est facile d'oublier.

Vous diriez que CaRE a bien structuré votre approche ?

Technicienne SI : Oui ! Avant, on n'avait pas cette feuille de route. CaRE, c'est clair et progressif : ça te donne des étapes à suivre, un cadre pour que rien ne passe à la trappe. Le domaine 1 nous a permis de poser les bases : gouvernance, rôles, plan de crise, etc. Maintenant, on attend le déploiement du domaine 2 pour renforcer les aspects techniques, ressortir les activités critiques pour formaliser le plan de continuité et de reprise de nos activités.

Vous anticipez des difficultés pour ce domaine 2 ?

Technicienne SI : Oui, forcément. C'est toujours plus dur de mobiliser les ressources pour la partie technique : ça demande du budget, des compétences, et ça prend du temps. On espère que les résultats des exercices de crise vont convaincre la direction d'investir dans ces mesures.

Qu'est-ce que vous retenez des points forts de CaRE jusqu'ici ?

Technicienne SI : Son côté structuré et concret. Et aussi le fait qu'il pousse à l'entraînement : on voit bien que les exercices sont essentiels. Même si ça prend du temps, ça nous met en conditions réelles et ça renforce la cohésion.

Et si vous deviez pointer des limites ou des points d'amélioration ?

Technicienne SI : Je dirais qu'il faut encore simplifier certains messages pour les équipes métiers. Le vocabulaire est parfois trop technique. Et puis, il faut que ça devienne un réflexe : aujourd'hui, on est encore trop dans la documentation, pas assez dans la mise en pratique continue.

[00:48:03 - 54,17]

Conclusion et perspectives

Finalement, si vous deviez résumer ce que vous avez appris à travers EBIOS et CaRE, ce serait quoi ?

Technicienne SI : Que la technique seule ne suffit pas. La préparation, c'est avant tout une question d'organisation et de communication. Et qu'il faut toujours s'adapter, parce qu'une crise cyber, ce n'est jamais exactement comme on l'imagine sur le papier.

Que recommanderiez-vous à un autre établissement pour mieux se préparer ?

Technicienne SI : De ne pas attendre l'attaque pour se poser les bonnes questions. De faire des exercices réguliers, même s'ils sont imparfaits. Et de faire participer tout le monde : les soignants, l'accueil, l'administratif… parce que la crise, elle concerne tout le monde, pas juste l'IT.

Merci beaucoup pour tous ces partages. Vous seriez d'accord pour que je revienne vers toi si besoin ?

Technicienne SI : Bien sûr ! Si je peux vous aider, ce sera avec plaisir.

Fin de l'entretien à 14h54.

Annexe 3 : entretien avec l'expert cyber & RSSI

Bonjour, et encore merci de me recevoir pour cet échange. Je travaille actuellement sur un mémoire centré sur la résilience des établissements de santé face aux cyberattaques. Ma problématique porte sur la manière dont le programme CaRE permet de mieux gérer ces crises, et sur ce que la méthode EBIOS peut apporter pour anticiper et gérer ces crises. Mon objectif aujourd'hui est donc de mieux comprendre comment votre solution Agile Risk Manager, qui intègre EBIOS, s'inscrit dans cette dynamique, et de recueillir vos retours d'expérience et votre regard d'expert sur les conditions de réussite d'une telle démarche. L'entretien devrait durer environ une heure. Si ça vous convient, je vous propose de commencer.

1. Contexte et démarche

Pour commencer, pourriez-vous me présenter ALL4TEC et votre outil Agile Risk Manager ?

Pourquoi avoir choisi de vous appuyer sur la méthode EBIOS, et comment l'avez-vous adaptée pour le secteur hospitalier ?

Expert Cyber : La méthode EBIOSRM est très largement utilisée en France pour les analyses de risque cyber, que ce soit sous son nom ou sous l'appellation ISO 27005, dont la version 2022 correspond à EBIOSRM. Elle est labellisée par l'ANSSI, et toutes les administrations publiques en France doivent l'appliquer pour leurs analyses de risque.

2. EBIOS appliqué au contexte hospitalier

Quels sont, selon vous, les apports concrets d'EBIOS pour prévenir les risques cyber dans les établissements de santé ?

Expert Cyber : Il est crucial de bien définir le périmètre de l'analyse de risque, surtout dans des structures complexes comme les hôpitaux, pour cibler les systèmes d'information essentiels. Nous devons identifier ces systèmes d'information essentiels dans les hôpitaux et réaliser des analyses de risque spécifiques pour chacun d'eux. La méthode EBIOS RM est souple, elle comprend cinq ateliers qui sont tous facultatifs, ce qui permet d'adapter l'analyse de risque aux besoins spécifiques.

Expert Cyber : Une de nos préoccupations est de communiquer les risques cyber de manière à ce qu'ils soient compris par les métiers et les décideurs, car avant, les communications étaient trop techniques et ne permettaient pas une bonne compréhension des enjeux. Il est prévu de définir les processus critiques liés aux urgences pour mieux comprendre les risques associés et les relier aux systèmes d'information nécessaires à leur gestion.

Expert Cyber : Je m'interroge aussi sur les conséquences d'une fuite d'informations de R&D, car cela pourrait entraîner des risques financiers importants et la possibilité de produire un vaccin dangereux, ce qui souligne l'importance de la sécurité des données dans le secteur de la santé. Il est primordial de comprendre le cadre législatif et les référentiels obligatoires dans la santé, et de s'assurer que toutes les règles sont bien appliquées pour éviter des failles de sécurité. L'évaluation de la gravité des événements redoutés est subjective, ce qui peut complexifier l'analyse des risques, d'où la nécessité d'une approche structurée pour classer ces événements.

Quels types de scénarios ou d'actifs critiques sont les plus souvent identifiés dans ce contexte ?

Expert Cyber: Les attaquants peuvent être très divers, des activistes aux groupes criminels, et les hôpitaux, par exemple, manquent souvent de visibilité sur le profil de l'attaquant. Je me demande si certaines de nos peurs concernant les menaces sont fondées ou non, ce qui soulève la question de l'importance de cibler les attaquants qui ont un intérêt réel pour l'organisation. Il y a environ 1200 à 1300 grandes attaques référencées chaque année en France, ce qui montre l'ampleur du problème de sécurité. Plus de 70% de ces grandes attaques en France proviennent de parties prenantes, ce qui souligne la nécessité d'une évaluation rigoureuse de ces acteurs.

Votre méthode aide-t-elle aussi à mieux gérer la crise une fois l'attaque en cours, ou est-elle uniquement préventive ?

Expert Cyber: Nous prévoyons de travailler avec des experts cyber lors de l'Atelier 4 pour approfondir les détails techniques des attaques et établir des mesures de sécurité appropriées. Il est crucial de comprendre les chemins d'attaque et les étapes qu'un attaquant suivrait, ce qui est essentiel pour la sécurité des systèmes d'information, surtout dans des environnements complexes comme les hôpitaux.

Expert Cyber : Je constate parfois que des mesures de sécurité sont mises en place sans réel sens dans de nombreux contextes, ce qui entraîne des dépenses inutiles. Environ 30% des mesures de sécurité proposées par les référentiels peuvent ne pas être pertinentes. L'ISO 2700-2, par exemple, comprend 93 ou 94 mesures de sécurité, et

j'estime qu'environ 30% d'entre elles ne sont pas adaptées à la plupart des contextes, ce qui soulève des questions sur l'efficacité des référentiels de sécurité.

3. Retours terrain et exemples

Avez-vous accompagné des établissements de santé ? Quels enseignements tirez-vous de ces expériences ?

Expert Cyber : Il n'existe pas de guide standard pour répondre aux cyberattaques, ce qui est une préoccupation majeure pour les établissements. Cependant, tous les centres hospitaliers de France sont actifs dans l'analyse des risques, ce qui montre une large adoption de cette pratique.

Quels sont, selon vous, les facteurs de réussite ou au contraire les blocages pour mettre en œuvre une vraie démarche de gestion des risques ?

Expert Cyber : Je recommande de commencer modestement avec des analyses de risque "flash", ce qui permet d'avoir rapidement une vision de la situation et de développer un plan de traitement sur quelques mois. Une analyse de risque peut être réalisée en un jour ou deux, permettant d'obtenir des résultats rapides et significatifs. Beaucoup d'établissements ne savent pas par où commencer leur analyse des risques, ce qui peut être un obstacle à la mise en œuvre de processus efficaces.

4. Lien possible avec CaRE

Avez-vous entendu parler du programme CaRE, porté par l'ANS pour renforcer la cybersécurité des établissements de santé ?

Expert Cyber : Oui, nous sommes d'accord que le Programme CaRE est principalement destiné aux petites structures et que l'analyse des risques doit être intégrée dans leur fonctionnement.

Voyez-vous des ponts possibles entre votre approche EBIOS et les démarches comme celles du Plan de Continuité et de Reprise d'Activité (PCRA) proposées dans ce programme ?

5. Vision et perspectives

Selon vous, comment la méthode EBIOS pourrait-elle évoluer pour mieux accompagner les hôpitaux dans les années à venir ?

Quels conseils donneriez-vous à un établissement qui souhaite entamer une démarche d'analyse de risques mais ne sait pas par où commencer ?

Expert Cyber : Je recommande de consulter un document d'analyse de risque disponible en libre téléchargement comme point de départ pour les établissements souhaitant commencer leur analyse des risques. Le guide EBIOS de l'ANSSI, qui fait 70 pages, est une ressource accessible et utile pour ceux qui s'engagent dans une analyse des risques.

Merci beaucoup pour cet échange très riche. Vos retours vont m'aider à mieux comprendre comment l'analyse de risque peut contribuer à la résilience des

établissements de santé, en particulier face aux menaces cyber. Encore merci pour votre disponibilité et votre partage d'expertise.

Fin de l'entretien à 10h01 (31 min)

HOUMADI Zaïdatte

DANS QUELLE MESURE LE PROGRAMME CYBERSÉCURITÉ ACCÉLÉRATION ET RÉSILIENCE DES ÉTABLISSEMENTS (CARE) PERMET-IL AUX ÉTABLISSEMENTS DE SANTÉ DE GÉRER LES CRISES LIÉES AUX CYBERATTAQUES ET QUELS ENSEIGNEMENTS TIRER DE LA MÉTHODE EBIOS RM POUR RENFORCER CETTE RÉSILIENCE ?

Le secteur de la santé, par la nature sensible de ses données et la criticité de ses activités, est devenu une cible privilégiée des cyberattaques, engendrant des impacts majeurs sur la continuité des soins et la sécurité des patients. Dans ce contexte de menaces croissantes, la gestion des crises cybernétiques et le renforcement de la résilience des établissements de santé sont devenus des enjeux stratégiques. Le programme Cybersécurité Accélération et Résilience des Établissements (CaRE) vise à outiller ces structures pour faire face à ces défis. Cependant, l'efficacité de tels programmes repose également sur une compréhension approfondie des risques et une capacité à les anticiper. Ce mémoire explore dans quelle mesure le programme CaRE permet aux établissements de santé de gérer efficacement les crises liées aux cyberattaques, et quels enseignements peuvent être tirés de la méthode EBIOS Risk Manager (EBIOS RM) pour renforcer cette résilience. L'application de la méthode EBIOS RM, en tant qu'outil d'analyse et de gestion des risques, est examinée pour son potentiel à améliorer la posture de sécurité et la préparation face aux incidents cyber.

Mots-clés : **cyberattaque, cybersécurité, santé, EBIOS RM, gestion de crise, programme CaRE, résilience**.

HOW DOES THE CYBERSECURITY ACCELERATION AND RESILIENCE FOR FACILITIES (CARE) PROGRAM HELP HEALTH FACILITIES MANAGE CYBERATTACK CRISES, AND WHAT CAN WE LEARN FROM THE EBIOS RM METHOD TO MAKE THEM STRONGER?

The healthcare sector, due to the sensitivity nature of its data and the criticality of its activities, has become a prime target for cyberattacks, leading to significant impacts on continuity of care and patient safety. In this context of growing threats, cybersecurity crisis management and the strengthening of healthcare institutions' resilience have become strategic imperatives. The Cybersecurity Acceleration and Resilience for Healthcare Facilities (CaRE) program aims to equip these structures to address these challenges. However, the effectiveness of such programs also relies on a deep understanding of risks and the ability to anticipate them. This thesis explores the extent to which the CaRE program enables healthcare institutions to effectively manage cyberattack-related crises, and what lessons can be learned from the EBIOS Risk Manager (EBIOS RM) method to enhance this resilience. The application of the EBIOS RM method, as a risk analysis and management tool, is examined for its potential to improve security posture and preparedness for cyber incidents.

Keywords: **cyberattack, cybersecurity, healthcare, EBIOS RM, crisis management, CaRE program, resilience**.