Adel TAOULI

Master 2 Audit interne des organisations

Année universitaire 2020-2021

IAE AIX Aix-Marseille Graduate School of Management
Aix*Marseille Université

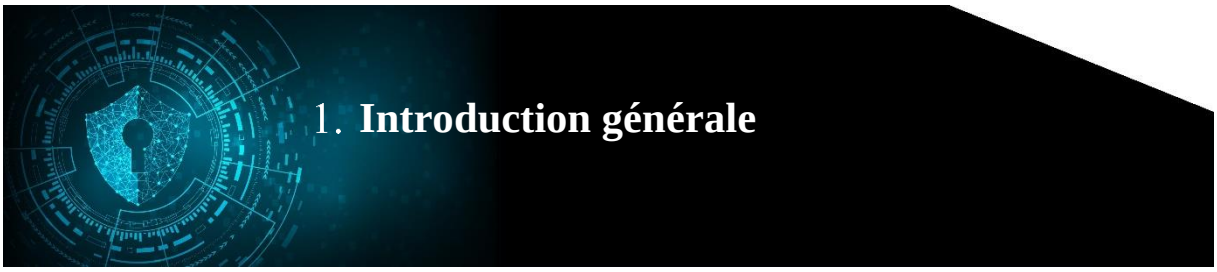
Remerciements

Je tiens à remercier M. Bono, directeur du programme MSc 2 Audit & Corporate Governance, ainsi que mon tuteur, M. Forestier, pour leur supervision dans le cadre de la rédaction de ce mémoire.

Je souhaite aussi remercier mes trois tuteurs, Claire Massé, Damo Konan et Stéphane Fabriès, qui m’ont accompagné lors de mes cinq années d’alternance. Leur confiance et leur bienveillance m’ont permis de m’épanouir professionnellement et de faire de mes débuts en entreprise une réussite.

Mes remerciements s’adressent enfin à l’ensemble de mes professeurs et des intervenants pour m’avoir conféré des enseignements de qualité et les meilleurs outils pour réussir mon insertion professionnelle.

Sommaire



1. Introduction générale

Dans la dernière enquête européenne annuelle « Risk in Focus 2021 » réalisée par l'ECIIA (European Confederation of Institutes of Internal Auditing) auprès de professionnels de l'audit interne, la cybersécurité et la protection des données figurent en tête du classement des principaux risques auxquelles sont confrontés les entreprises. Près de 79 % des responsables d'audit interne interrogés considèrent les cyber-risques comme étant le type de risque le plus important auxquels ils doivent faire face. Cette étude révèle que la cybersécurité est devenue un véritable enjeu pour les organisations dont la responsabilité ne se limite plus seulement aux services informatiques. L'auditeur interne, acteur privilégié du processus de management des risques, a vu ses fonctions évoluer pour devenir un véritable collaborateur clé dans la mitigation des cyber-risques. La technicité inhérente à ce thème ainsi que son importance aux yeux des dirigeants qui ne cessent tous deux de s'accroitre requiert de l'auditeur interne l'acquisition de nouvelles compétences clés afin de pouvoir continuer à assurer ses fonctions. C'est dans cette logique que s'inscrit le choix de mon sujet. En effet, étant conscient de l'importance actuelle et grandissante pour le futur des enjeux liés à la cybersécurité pour les organisations, je souhaite profiter de ce mémoire pour développer une véritable expertise dans cette thématique. En parallèle de cet exercice de recherche, j'ai entrepris une formation au CNAM qui m'a permis d'obtenir un certificat de spécialisation en audit des systèmes d'information.

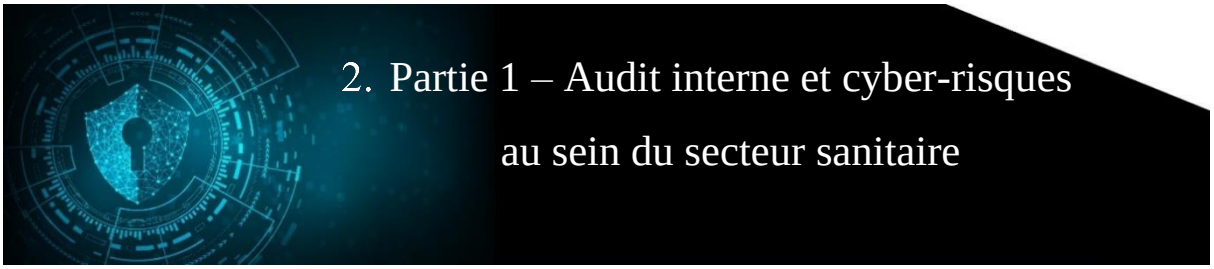
Afin de rendre ce mémoire mobilisable dans un cadre professionnel, une approche sectorielle sera privilégiée. Le sujet sera donc étudié en étant appliqué au secteur sanitaire. Ayant travaillé durant trois années au sein de ce secteur, j'ai naturellement décidé d'axer mon mémoire sur celui-ci. Le secteur de la santé s'illustre par la place privilégiée qu'il accorde à l'humain ainsi que la grande diversité de ses métiers. J'ai pour objectif de réintégrer ce secteur après ma

prochaine expérience en audit financier, ce qui rend le sujet particulièrement intéressant à mes yeux. De plus, la cybersécurité est une réelle problématique dans ce secteur qui est une cible privilégiée des criminels du fait du traitement de données sensibles inhérent à l'activité ainsi que du manque de ressources auquel doivent faire face les acteurs en charge de la sécurité informatique.

Ce mémoire permettra de répondre à la problématique suivante : **quel rôle l'audit interne doit-il jouer dans la mitigation des risques liés aux cyberattaques au sein du secteur sanitaire ?**

Le principal objectif de ce mémoire sera de déterminer le rôle de l'audit interne dans la gestion des cyber-risques au sein des structures sanitaires et de proposer un guide d'audit de la cybersécurité qui permettra de se prévenir au mieux de potentielles attaques et de limiter leurs conséquences le cas échéant. Pour cela, ce mémoire se propose de faire la lumière sur les principales notions clés liées à la cybercriminalité ainsi que les enjeux afférents pour les organisations, et en particulier celles du secteur de la santé avec leurs spécificités. Le rôle grandissant de l'audit interne dans le processus de gestion des cyber-risques sera étudié afin de pouvoir déterminer la démarche méthodique qu'il lui est nécessaire d'adopter.

Le principal apport de ce mémoire résidera dans la proposition de guide méthodologique d'audit de la cybersécurité appliqué à une organisation sanitaire, qui, par son approche systématique et méthodique, reprendra l'ensemble des étapes de la mission afin de les expliciter. Afin d'illustrer de manière pratique l'application de la proposition de méthodologie, un exemple fictif de structure sanitaire sera utilisé.



2. Partie 1 – Audit interne et cyber-risques au sein du secteur sanitaire

2.1. La notion de cybercriminalité : tendances, mécanismes et conséquences

2.1.1. La cybercriminalité, un risque majeur pour les entreprises

2.1.1.1. La cybercriminalité, une notion encore nouvelle

La révolution numérique qui s'opère depuis quelques décennies a permis de démocratiser l'accès à l'informatique ainsi que la globalisation des réseaux. C'est dans ce contexte qu'une nouvelle forme d'infraction a vu le jour : la cybercriminalité. Bien que ce terme soit largement utilisé de nos jours, la cybercriminalité ne bénéficie pas d'une définition exacte et partagée. En l'absence d'une définition unanimement admise, plusieurs États ont développé leur propre définition afin de l'intégrer à leur législation. En Angleterre, le Service des Procureurs de la Couronne a publié une note d'orientation qui propose la définition suivante de la notion traitée : *« la cybercriminalité est un terme générique utilisé pour décrire deux types d'infraction :*

- *Les infractions spécifiques aux technologies de l'information et de la communication : vol de données, fraude à la carte bancaire… ;*
- *Les infractions facilitées par les technologies de l'information et de la communication : escroquerie en ligne, blanchiment d'argent…* »[1].

Aux États-Unis, les États fédérés ont aussi développé leur propre définition de la notion de cybercriminalité de manière indépendante. Le Code pénal du Texas désigne la cybercriminalité comme le fait *« d'accéder à un ordinateur, à un réseau, ou à un réseau informatique sans avoir l'autorisation de son propriétaire* »[2]. Le Code pénal de la Virginie-Occidentale définit lui la cybercriminalité comme le fait « *d'accéder ou de permettre d'accéder sciemment*

[1] « Cybercrime – prosecution guidance », publié le 26 septembre 2019.
[2] Section 33.02 du Code pénal de l'État de Californie

et délibérément à un ordinateur ou à un réseau informatique, de manière directe ou indirecte, dans l'objectif :

- *De procéder à tout stratagème ou artifice afin de frauder ;*
- *D'obtenir de l'argent, des biens ou des services au moyen de prétextes ou promesses frauduleuses* »[3].

En France, ce type d'infraction n'est aujourd'hui pas défini légalement, le mot « cybercriminalité » ne figure pas dans le Code pénal. Pour autant, certaines structures rattachées au Gouvernement ont pu travailler sur l'élaboration d'une définition. C'est le cas de l'autorité nationale en matière de sécurité et de défense des systèmes d'information représentée par l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) qui définit la cybercriminalité comme « *[tous] actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyen de réalisation d'un délit ou d'un crime, ou les ayant pour cible* »[4].

Avec la pléthore de définitions disponibles, le terme peut paraitre difficile à conceptualiser au premier abord. Son caractère protéiforme lui permet en effet de recouvrir une grande variété d'infractions. Afin de faciliter la compréhension de ce mémoire, la définition suivante de la notion traitée sera utilisée : la cybercriminalité désigne toute infraction perpétrée au moyen d'un système d'information interconnecté à un réseau de télécommunication. Cette définition, élaborée à partir des recherches réalisées, reste assez large afin de pallier le caractère protéiforme du terme et correspondre au sujet traité dans le cadre de ce mémoire. Les cyber-risques désignent quant à eux les conséquences que peuvent avoir les cyber-attaques.

La difficulté à définir cette notion peut aussi s'expliquer par son caractère encore récent. En effet, le premier acte de cybercriminalité recensé en tant que tel ne date que des années 70. À cette époque, John Draper, alias « Captain Crunch » découvre qu'un sifflet obtenu dans une boite de céréales de la marque Cap'n Crunch émet un son à 2600 Hz qui permet directement d'interagir avec la centrale de la compagnie téléphonique Bell. En se connectant au réseau de la centrale,

[3] Chapitre 61-3C-4 du Code pénal de la Virginie-Occidentale
[4] Disponible sur https://www.ssi.gouv.fr/entreprise/glossaire/c/

John pouvait alors passer des appels longue distance de manière totalement gratuite. Le « *Phreaking* »[5] était alors né.

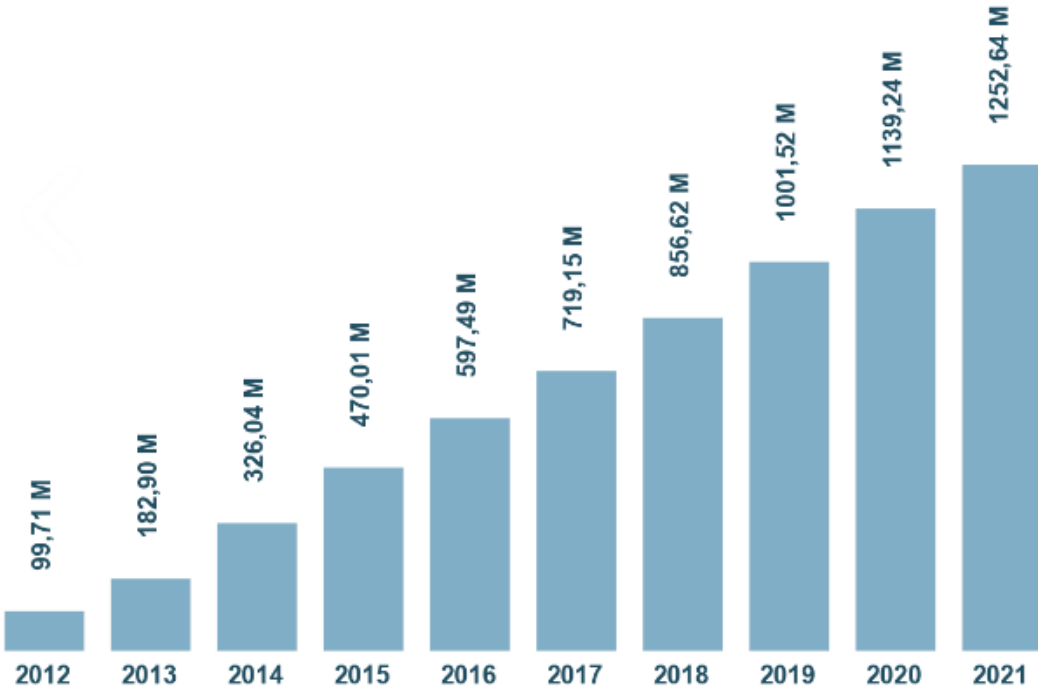
Ce n'est qu'en 1988 que Morris Worm devient la première personne inculpée pour crime informatique. Alors étudiant à l'université Cornell, Morris code un logiciel qui a objectif de se transmettre via internet aux ordinateurs connectés afin de se répandre massivement. Bien qu'étant initialement inoffensif, le logiciel va contaminer des milliers d'ordinateurs et les rendre inutilisables à cause d'une erreur de codage, devenant ainsi le premier vers informatique. Morris sera alors condamné à 400 heures de travaux d'intérêt général. Après cet événement, une prise de conscience va peu à peu se faire autour de l'importance de la cybersécurité et de ses enjeux. Quelques jours après l'attaque, la première équipe d'intervention d'urgence informatique va être créée au sein du Département de Défense des États-Unis.

2.1.1.2. Un phénomène en pleine expansion

Depuis ces quelques actes isolés, les actes de cybercriminalité n'ont cessé d'augmenter avec des conséquences de plus en plus importantes. L'usage d'outils de piratage est devenu de plus en plus accessible, avec l'apparition de logiciels prêts à l'emploi. Une des techniques les plus utilisées par les cybercriminels consiste à infecter un ordinateur ou un réseau à l'aide d'un logiciel malveillant. En 2021, l'entreprise Av Test GmBh spécialisée dans la cybersécurité a recensé plus d'un milliard de logiciels de ce type dans le monde, un chiffre qui a été multiplié par près de 12 en l'espace de 10 ans (figure 1 ci-après).

[5] Contraction de « phone » (téléphone en anglais) et hacking (piratage en anglais)

Figure 1 : évolution du nombre de logiciels malveillants recensés (en millions)

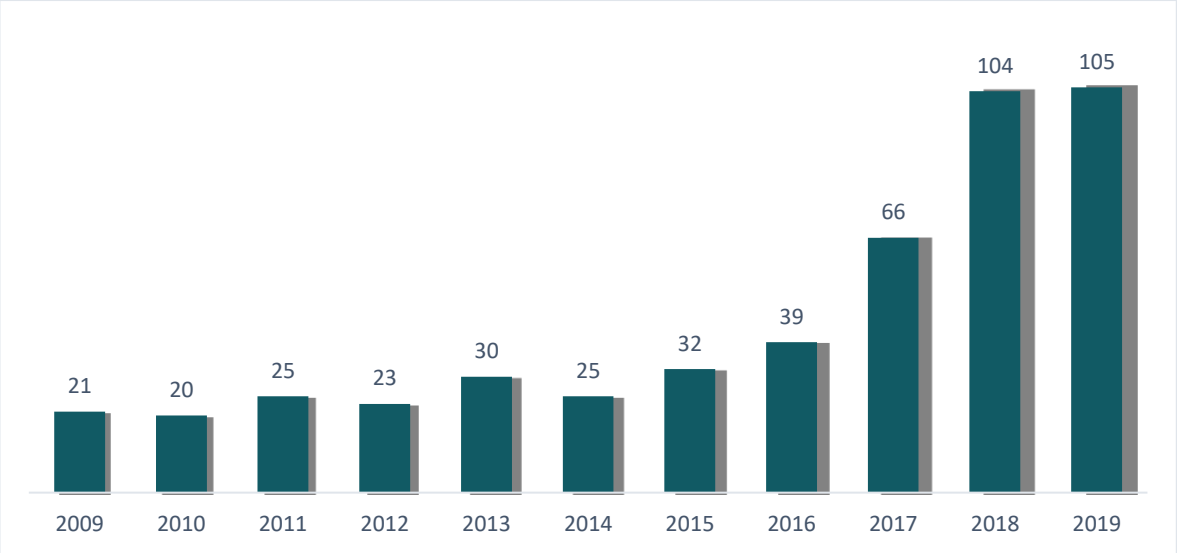


Source : Av Test GMBH, Statistiques 2021.

Les conséquences de ces attaques peuvent entrainer des pertes de plusieurs millions de dollars pour les plus grosses compagnies (figure 2 ci-après). Des multinationales comme Apple, Uber ou encore Nintendo ont vu les données de plusieurs millions de leurs clients se faire voler pour ensuite être mises sur Internet. Une étude menée par l'entreprise McAfee et le Centre d'études stratégiques et internationales (CSIS) estime à mille milliards de dollars les coûts imputables aux attaques informatiques en 2020, soit plus de 1 % du PIB mondial[6]. C'est dans ce contexte que les entreprises investissent de plus en plus dans la cybersécurité de leurs infrastructures afin de se protéger des intrusions. Selon le cabinet de conseil Gartner, référence dans ce secteur d'activité, le marché de la cybersécurité va continuer de croître à hauteur de 12,4 % en 2021 pour atteindre près de 150 milliards, après une hausse de 6,4 % en 2020 [7].

[6] The hidden costs of cybercrime, 2020, McAfee.
[7] Disponible sur https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Figure 2 : évolution du nombre d'incidents reportés liés à des cyberattaques ayant causés une perte supérieure à 1 million de dollars aux États-Unis



Source : Federal Bureau of Investigation's Internet Crime Complaint Center.

2.1.1.3. Une menace réelle pour toutes les entreprises

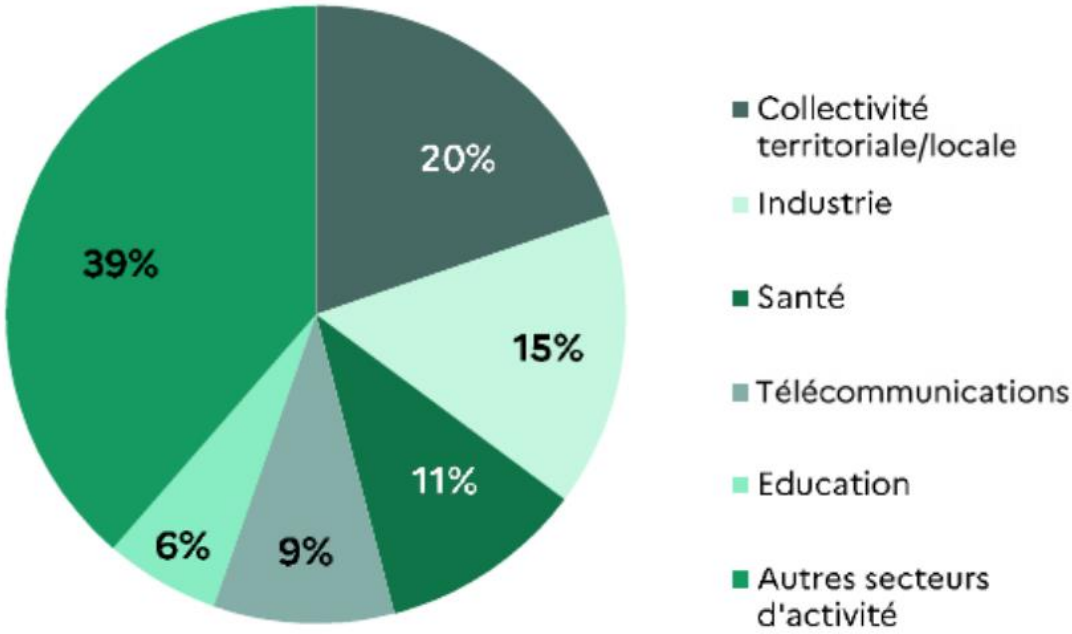
La cybercriminalité touche tous les secteurs d'activités, aucune entreprise n'est à l'abri. Pour exemple, le 8 décembre 2008, le spécialiste américain de la cybersécurité FireEye, dont les principaux clients sont des administrations publiques des États-Unis, a annoncé avoir été piraté par un criminel qui leur a dérobé leurs logiciels d'attaques. En France, selon une étude menée par l'assureur Hiscox, près de la moitié des entreprises françaises ont subi une cyberattaque en 2021 [8]. Aucun secteur n'est épargné, mais certains sont particulièrement visés. C'est le cas du secteur de la finance, et en particulier des structures bancaires qui représentent de véritables mines d'informations sensibles comme les numéros de cartes bancaires. Les organismes publics sont aussi des cibles de choix pour les cybercriminels, car ils possèdent de larges volumes de données confidentielles protégés par des infrastructures technologiques qui peuvent parfois être obsolètes. Le secteur de la santé est aussi particulièrement touché du fait du traitement de données sensibles inhérent à son activité et au manque d'investissement dans la cybersécurité. Selon l'Agence Nationale de la Sécurité des Systèmes

[8] Rapport Hiscox 2021 sur la gestion des cyber-risques.

d'informations, le secteur public et le secteur de la santé représentent respectivement 20 % et 15 % du total des cyberattaques subies en France en 2020 à l'aide de rançongiciels (figure 3 ci-après).

Bien que les piratages de grandes sociétés soient particulièrement médiatisés, les PME restent les cibles privilégiées des cybercriminels. En effet, selon DAF Magazine, 77 % des cyberattaques ciblent les PME. Pour les entreprises touchées, 60 % des PME impactées par une cyberattaque font faillite dans les 6 mois [9].

Figure 3 : Secteurs d'activités touchés par les rançongiciels en 2020 en France



Source : ANSSI, Cybersécurité, faire face à la menace : la stratégie française

[9] Disponible sur https://www.daf-mag.fr/Thematique/gestion-risque-1241/Infographies/Cyberattaques-attaques-concernent-PME-304616.htm

2.1.2. **Panorama de la cybercriminalité en entreprise**

2.1.2.1. Profils des cybercriminels

Avant de commencer à décortiquer les profils des cybercriminels, il est nécessaire de faire tout d'abord la distinction entre les deux grandes catégories de pirates informatiques : les *White Hat* (en français : chapeau blanc) et les *Black Hat* (en français : chapeau noir). Les *White Hat*, ou hackers éthiques, sont des pirates informatiques ou des experts en cybersécurité qui testent la robustesse du système de sécurité d'une entreprise avec sa permission afin d'en déterminer les failles et de les reporter. Les *Black Hat* sont quant à eux des pirates informatiques mal intentionnés qui agissent dans l'objectif de tirer un bénéfice financier ou bien de nuire à des individus ou à des organisations. Cette distinction, bien que quelque peu binaire, permet tout de même de différencier deux catégories de pirates informatiques, qui bien qu'ils utilisent des procédés similaires, agissent à des fins différentes. Du fait de son sujet, ce mémoire se concentrera naturellement sur les pirates dits *Black Hat*.

Selon le benchmark réalisé par Wavestone sur les incidents de sécurité pour l'année 2020 en France, près de 50 % des cyberattaquants agissent en groupe. 30 % d'entre eux agissent même de manière quasi professionnelle avec le développement en interne de leurs propres outils et seulement 24 % sont des cybercriminels agissant de manière indépendante (figure 4 ci-après).

Une autre étude menée par les sociétés Thalès et Verint sur 66 groupes de pirates informatiques a permis de faire ressortir 4 grandes catégories de cyberattaquants (figure 5 ci-après) [10] :

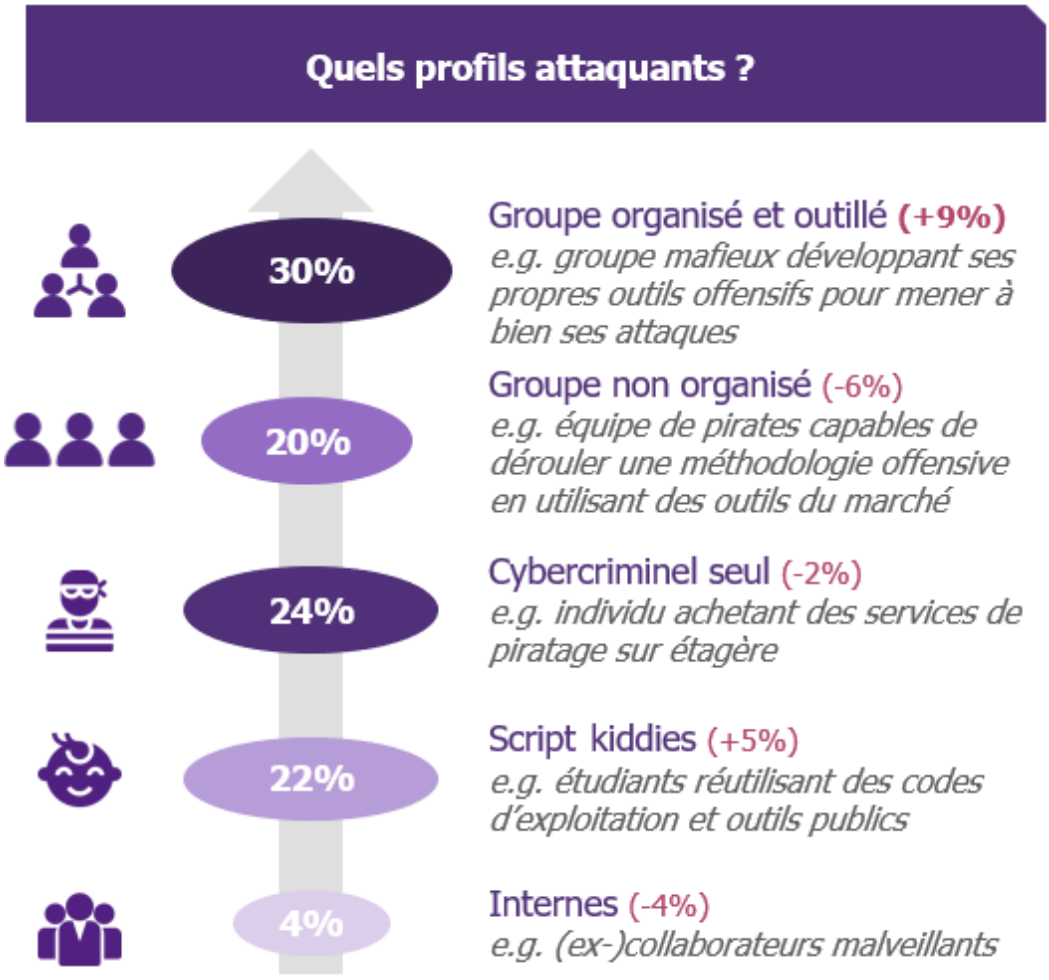
- Les pirates parrainés par des États qui représentent près de 49 % des attaquants et qui se concentrent sur le vol de données sensibles de cibles géopolitiques ;
- Les cyberactivistes (26 %) qui poursuivent des motivations idéologiques et qui œuvrent à des fins d'atteinte à l'image de leur cible ;
- Les cybercriminels (20 %) qui visent le gain financier ;
- Les cyberterroristes (5 %) qui ont pour objectif de détruire les données de leurs victimes.

[10] The Cyberthreat handbook, octobre 2019, Thalès & Vérint.

Le profil qui nous intéresse le plus ici est celui des cybercriminels, car c'est celui qui correspond au sujet traité. En effet, ce sont eux qui visent tous les types d'entreprises, et cela peu importe leur secteur d'activité, toujours dans l'objectif d'en tirer un bénéfice financier.

Au niveau géographique, selon une étude menée par le groupe NTT spécialisé dans la collecte et l'analyse de données relatives à la sécurité informatique, les cyberattaques proviennent principalement des États-Unis (22 %), de la Chine (13 %), du Japon (6 %) et de la France (5 %) [11]. Ces données peuvent être corrélées avec le niveau d'éducation de la population et la qualité des infrastructures techniques du pays.

Figure 4 : profils des cyberattaquants



Source : Cyberattaques en France : quelle situation sur le terrain ?, 2020, Wavestone.

[11] 2019 Global Threat Intelligence Report, NTT.

Figure 5 : profils des pirates informatiques

Source : The Cyberthreat handbook, octobre 2019, Thalès & Vérint.

2.1.2.2. Les différents mécanismes employés par les cybercriminels

Cette partie consistera à dresser un panorama des principaux mécanismes informatiques utilisés par les cybercriminels contre les entreprises afin de parvenir à leurs fins. Il convient ici de préciser que la plupart des cyberattaques sont dues au facteur humain. En effet, les cybercriminels utilisent **l'ingénierie sociale** qui consiste à manipuler l'individu à des fins d'escroquerie.

Le terme « **programme malveillant** » ou ***malware*** est un terme générique qui désigne tout type de logiciel malveillant visant à s'infiltrer dans un appareil informatique. L'utilisateur va télécharger le logiciel sans s'en rendre compte en cliquant sur un lien ou sur une pièce jointe qui une fois installée va ensuite bloquer le système ou l'accès à certains composants, ou récupérer et transmettre des informations de l'appareil. Le type de *malware* le plus utilisé est le *ransomware* (rançongiciel en français). Selon le guide publié par l'organisme gouvernemental Cybermalveillance et Bpifrance, le *ransomware* représente à lui seul 22 % du volume total des cyberattaques [12]. Celui-ci va bloquer l'accès à l'ordinateur ou à

[12] Guide cybersécurité à destination des dirigeants des TPE, PME, ETI. Bpifrance & Cybermalveillance.gouv.fr.

ses fichiers en les chiffrant et en réclamant le paiement d'une rançon afin de rétablir l'accès.

Le ***phising*** (hameçonnage en français) consiste à se faire passer pour un tiers de confiance via un e-mail, SMS ou appel téléphonique afin de récupérer des informations personnelles ou professionnelles à des fins frauduleuses. La technique de *phising* la plus répandue est l'envoi d'un e-mail semblant provenir d'une personne de confiance qui va rediriger la victime vers un site web frauduleux où elle va se voir demander ses informations de connexion et son numéro de carte bancaire.

L'attaque par **Déni de Service Distribué (DDos)** vise à rendre indisponible le serveur d'un site web, un service ou une infrastructure en l'inondant de fausses demandes. De cette manière, le système attaqué n'est plus en mesure de répondre aux demandes légitimes.

Les attaques de type « **Man in the middle** » (l'homme au milieu en français) consistent à intercepter les échanges entre deux parties afin de s'immiscer dans la transaction. Dans ce procédé, l'attaquant a non seulement la possibilité de lire les messages échangés, mais aussi de les modifier en se faisant passer pour l'un, voire les deux correspondants.

L'injection SQL, *Structure Query Langage* (en français : langage de requête structurée) permet au pirate informatique d'injecter un morceau de code afin de manipuler une base de données et accéder à ses informations.

Le **téléchargement furtif** désigne le téléchargement involontaire de logiciels malveillants. Le cybercriminel intègre le logiciel dans un site, un courriel ou une pièce jointe afin d'infecter l'ordinateur de la cible. À la différence des autres types d'attaques, le téléchargement furtif ne nécessite pas qu'un utilisateur déclenche activement l'attaque, le pirate informatique peut profiter d'une faille de sécurité d'une application, d'un système d'exploitation, d'un navigateur web ou de ses extensions.

L'attaque par mot de passe consiste à utiliser un logiciel qui va essayer de deviner le mot de passe en testant des combinaisons à la suite. Une attaque par force brute va consister à tester de manière exhaustive les options possibles, ce qui est particulièrement efficace pour les mots de passe courts, contrairement à l'attaque par dictionnaire qui va consister à tester une série de mots potentiels à base d'une liste prédéfinie.

2.1.3. Les conséquences de la cybercriminalité pour les entreprises

2.1.3.1. Les conséquences financières

Le coût moyen d'une cyberattaque est aujourd'hui de 4,24 millions de dollars à l'échelle mondiale, selon la dernière étude d'IBM Security [13]. Afin de déterminer ce chiffre, 537 entreprises de pays, de tailles et d'activités différentes ont été analysées. Ce chiffre, qui peut paraître faramineux, reste une moyenne dont le défaut est d'être sensible aux valeurs extrêmes.

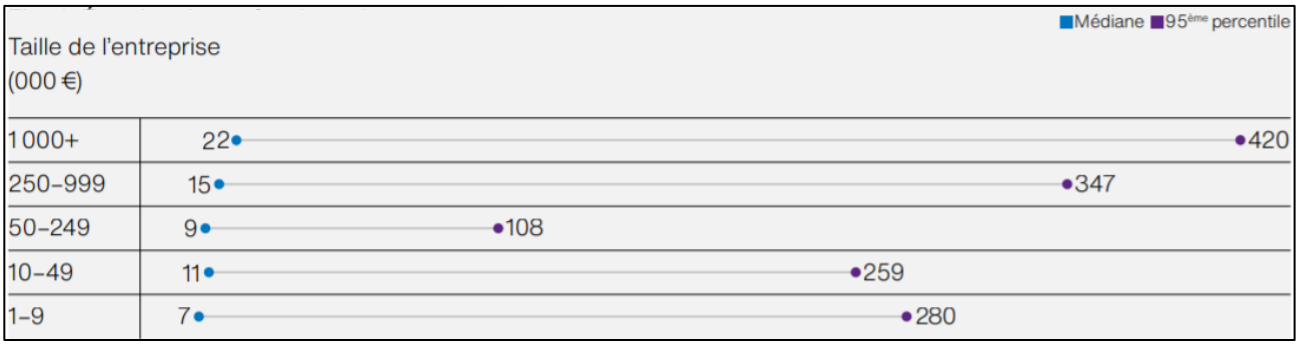
L'étude menée par l'assureur Hiscox permet d'avoir une vision plus précise du coût des cyberattaques en France (figure 5 ci-après). La disposition de ce graphique permet d'apprécier l'éloignement entre la valeur médiane, qui représente le point central des données, et le 95è percentile de chaque taille. Le premier constat en observant ce graphique est la disparité des conséquences financières pour toutes les catégories d'entreprises. Pour les entreprises de moins de 10 salariés, le coût médian de l'ensemble des attaques est environ 7 000 € contre 280 000 € au 95è percentile. Du côté des grandes entreprises de plus de 1000 salaries, la moitié des entreprises ont essuyé des pertes d'environ 22 000 € contre 420 000 € au 95è percentile.

Dans une étude menée par le cabinet Deloitte [14], 14 impacts financiers causés par une cyberattaque ont été répertoriés et répartis en deux catégories : les coûts connus et les coûts cachés. Parmi les coûts connus, qui ont la particularité d'être sur le court et moyen terme, l'amélioration des dispositifs de cybersécurité représente l'investissement nécessaire le plus important avec 1,25 % du montant total des dommages liés à la cyberattaque. Au niveau des coûts cachés, qui sont eux davantage sur le moyen et long terme, l'érosion du chiffre d'affaires lié à la perte de clients représente près de 50 % du montant total des dommages. Il est important de noter que les conséquences financières peuvent continuer à être subies près de 5 ans après la cyberattaque.

Une conclusion peut donc être établie ; les coûts d'une cyberattaque peuvent être très différents d'un cas à l'autre, mais ils peuvent néanmoins atteindre des sommes très importantes susceptibles de compromettre l'activité de l'entreprise.

[13] Cost of a Data Breach, IBM, 2021.
[14] Beneath the surface of a cyberattack, a deeper look at business impacts, Deloitte.

Figure 6 : étendue des coûts des cyberattaques



Source : rapport Hiscox 2021 sur la gestion des cyber-risques.

2.1.3.2. Les conséquences extra-financières

Les conséquences financières, qui ont l'avantage d'être quantifiables, sont seulement la partie émergée de l'iceberg. Selon la même étude évoquée déjà précédemment menée par le cabinet Deloitte, les dégâts immatériels causés par une cyberattaque représentent près de 40 % des dommages subis. En effet, en plus des coûts financiers directement imputables à l'incident, on peut répertorier les conséquences suivantes :

- Une interruption d'activité plus ou moins longue en fonction de la gravité de la cyberattaque ;
- L'atteinte à l'image de marque de l'entreprise ;
- La perte de confiance des clients au niveau commercial ;
- Des pertes de données (clients, fournisseurs…) ;
- Des poursuites judiciaires en cas de non-conformité aux exigences en termes de sécurité.

2.1.4. **Les moyens de protection contre les cyberattaques**

2.1.4.1. Les acteurs en charge de la cybersécurité en entreprise

Garantir la cybersécurité relève de la responsabilité de plusieurs acteurs au sein d'une entreprise. C'est un sujet qui doit tout d'abord être porté par la direction générale avant de pouvoir être décliné au niveau opérationnel. La direction doit pouvoir mettre à disposition de la Direction des Systèmes d'Information (DSI) des moyens adaptés afin de pouvoir protéger l'entreprise. Le directeur des systèmes

d'information pilote ensuite la politique de sécurité globale de l'entreprise. Le responsable de la sécurité des systèmes d'information viendra enfin la décliner au niveau opérationnel avec éventuellement d'autres collaborateurs sous sa responsabilité pour l'aider dans cette tâche. Ce dernier maillon aura la charge de surveiller l'application de la politique et des procédures de sécurité. Quand l'organisation n'a pas une taille suffisante pour supporter les fonctions décrites, c'est le directeur général ou le directeur des systèmes d'information, s'il existe, qui devra assumer ces responsabilités ou procéder à un arbitrage pour externaliser certaines activités.

Bien que le sujet doive avant tout être porté par les acteurs recensés ci-dessus, il convient de préciser que la cybersécurité est bien l'affaire de tous en entreprise. Il est communément admis que la cybersécurité n'est pas aussi puissante que son maillon le plus faible. En effet, la politique de sécurité la plus aboutie n'aura d'utilité si elle n'est pas respectée au niveau opérationnel par les collaborateurs. Tous les collaborateurs doivent être sensibilisés à cette thématique afin d'assurer une bonne hygiène informatique au niveau de l'entreprise.

2.1.4.2. Se protéger des cyberattaques

Afin de se protéger contre les cyberattaques, divers moyens de protection peuvent être déployés au sein d'une entreprise. Une réponse adaptée à la cybermenace sera composée de 3 grandes parties : la prévention, la détection et la protection des actifs informatiques. Le processus suivant, établi à partir des éléments de recherche, reprend les grandes étapes à suivre dans la gestion de la cybermenace. Il permet de limiter le risque d'une cyberattaque et de se protéger afin d'en limiter les conséquences le cas échéant.

Processus de gestion des cyberattaques.

Prévention

1. Sensibiliser les collaborateurs.
2. Gérer les mots de passe de l'entreprise : longueur minimum imposé de 8 caractères de types différents, changements réguliers obligatoires...
3. Mettre à jour les appareils, les logiciels et les antivirus.
4. Effectuer des sauvegardes régulières des données de l'entreprise.
5. Souscrire une assurance cyber-risque.

Détection

6. Procéder régulièrement à des analyses de sécurité du parc informatique
7. Installer un outil de détection d'intrusion.
8. Alerter les collaborateurs et la direction en cas d'intrusion avérée.

Protection

9. Déconnecter les machines compromises.
10. Rechercher les traces de compromission.
11. Déclencher le Plan de Continuité de l'Activité (PCA).
12. Déclarer le sinistre à l'assureur ainsi qu'à la CNIL et aller porter plainte.

2.1.4.3. L'importance de la cyber-résilience

Selon le cabinet EY, la cyber-résilience peut être définie comme « la capacité de détecter, résister, répondre ainsi que de se rétablir d'une cyberattaque dans un délai raisonnable » [15]. L'image du roseau, qui fait preuve de souplesse face au vent avant de revenir à sa position d'origine, est souvent utilisée pour expliquer la notion de résilience. Afin de pouvoir faire face à la cybermenace, les entreprises doivent, en amont, élaborer une stratégie de cyber-résilience pour permettre au système d'information de fonctionner à nouveau sous un certain délai. En effet, essayer de se prévenir du risque n'est plus suffisant, il est devenu nécessaire de se préparer au pire cas de figure afin de pouvoir réagir de la bonne manière en cas d'attaque avérée. Les entreprises qui savent faire preuve de cyber-résilience peuvent ainsi parvenir à évoluer dans un contexte de menaces persistantes et d'attaques complexes. Elles sont capables d'assurer la continuité de l'activité métier, même en mode dégradé, et de revenir à un fonctionnement normal dans les plus brefs délais. La cyber-résilience représente donc l'évolution logique que doit entreprendre la cybersécurité.

2.2. L'audit interne : une fonction en pleine mutation devenue une clé dans la gestion des cyber-risques

2.2.1. Un métier en évolution

2.2.1.1. L'audit interne, médecin de l'entreprise

« *L'audit interne, c'est tout ce que devrait faire un responsable pour s'assurer de la bonne maîtrise de ses affaires s'il en avait le temps, et s'il savait comment s'y prendre*. » Théorie et pratique de l'audit interne, Chap. 3 : un peu d'humour, 2010, Jacques Renard.

Selon la définition française validée par l'Institut Français de l'Audit et du Contrôle Interne (IFACI), l'audit interne « *est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise des*

[15] Disponible sur https://www.ey.com/en_lu/cybersecurity/cybersecurite---la-resilience--un-incontournable

opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée.
Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. »
Bien loin de la vision que l'on peut lui prêter, l'audit interne ne se limite pas seulement au contrôle, mais contribue à créer de la *valeur ajoutée* en *évaluant* et en *améliorant*. Véritable médecin de l'entreprise, l'audit interne intervient sur mandat de la direction afin de déceler les problèmes et formuler des recommandations. Afin d'assurer son indépendance, la fonction doit idéalement être rattachée au comité d'audit s'il existe, ou à la direction générale.

2.2.1.2. Une fonction comptable à l'origine…

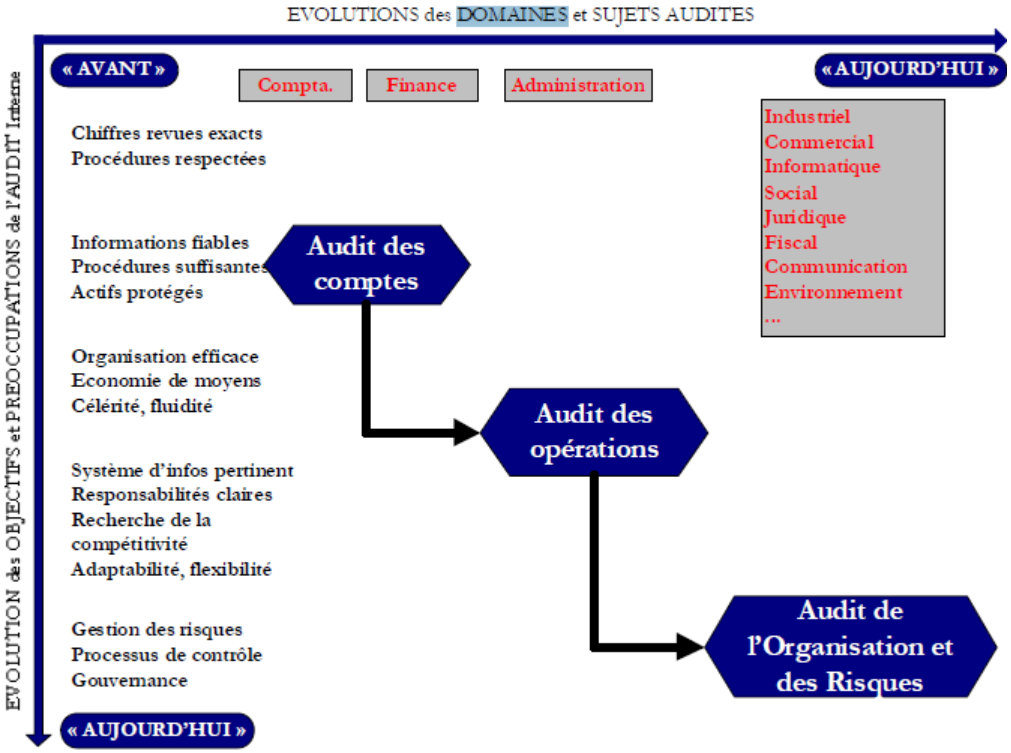
L'audit interne a longtemps été considéré comme une fonction de contrôle et de surveillance. La fonction était assimilée à un « chien de garde » (Morgan, 1979) qui agissait comme une police pour le compte de la direction générale. Né en 1930 aux États-Unis, l'audit interne était initialement restreint au domaine purement financier. La profession a été officiellement institutionnalisée en 1940 avec la création de *l'Institute of Internal Auditors* (en français l'institut des auditeurs internes). La fonction réalisait alors uniquement des missions d'audit d'assurance visant à évaluer le niveau de maîtrise des risques de l'objet audité. L'audit interne était le contrôle des contrôles (Candau, 1985) qui avait pour mission la vérification comptable (Mikol, 2020). L'audit interne n'était alors perçu que comme une extension de l'audit externe avec un champ d'action limité vis-à-vis de l'ensemble du management (Moeller & Witt, 1999). À partir de la création de l'IAA, l'audit interne n'a cessé d'évoluer et d'élargir ses fonctions.

2.2.1.1. …Devenue une fonction de véritable conseil stratégique

L'institutionnalisation de la fonction et les nombreux scandales financiers des années 2000 ont permis à l'auditeur interne d'évoluer afin de devenir un véritable

conseiller stratégique au service de la gouvernance. L'auditeur interne intervient maintenant sur l'ensemble des activités, fonctions et processus de l'organisation (Sillero, 2002). Dans son ouvrage publié en 2020, Pierre Schick reprend les principales évolutions de la fonction (figure 7 ci-après), de l'audit des comptes à l'audit des opérations, la fonction doit maintenant avoir la capacité d'évaluer l'ensemble de l'organisation et de ses risques. Dans ce contexte de plus en plus exigeant pour la profession, l'auditeur interne doit faire évoluer ses compétences afin de pouvoir pleinement continuer à assurer ses fonctions.

Figure 7 : évolution de l'audit interne



Source : PSK – Audit interne et référentiels de risques, 2020.

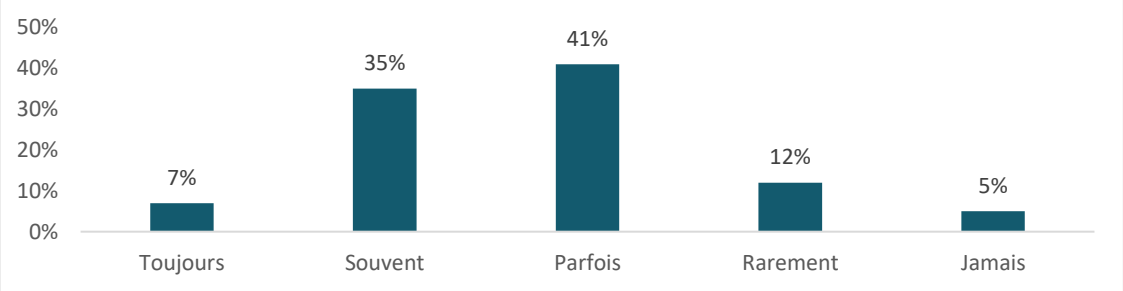
2.2.2. Vers un audit 2.0

2.2.2.1. Une mutation de la fonction obligée par la transformation numérique

Dans un contexte de profonde mutation des entreprises et de leur organisation provoquée par la révolution numérique, l'audit interne est lui aussi amené à évoluer. En effet, rester dans un modèle traditionnel d'audit interne expose la fonction au risque de perdre sa pertinence et sa valeur ajoutée. Les nouvelles

technologies représentent une opportunité pour la profession. Les outils d'analyses de données permettent désormais de traiter des volumes de données très significatifs. Les logiciels de visualisation des données ont eux aussi évolué avec une prise en main facilitée et des rendus graphiques plus intuitifs. Ces outils sont de plus en plus utilisés au sein des services d'audit internes. 62 % des fonctions disent avoir implanté des techniques d'analyse de données [16]. Leur principal avantage réside dans la possibilité de se passer de techniques de sondage pour avoir une lecture exhaustive de l'ensemble des données. Grâce à eux, on peut envisager de mettre en place un audit en continu permettant de capter et de traiter des données provenant des processus de l'entreprise de manière interrompue. Dans une étude menée par l'IIA aux États-Unis, seulement 5 % des auditeurs internes sondés affirment ne jamais utiliser l'analyse de données massives (figure 8 ci-après). Bien qu'ils ne soient pas encore incontournables, ces nouveaux outils pourraient bien le devenir dans un futur proche. L'évolution logique de ces outils serait l'implémentation de l'intelligence artificielle au cœur de l'audit interne. La convergence inévitable entre l'analyse de données et l'intelligence artificielle permettra d'envisager un audit prédictif. Les analyses descriptives basées sur ce qui s'est déjà passé seraient alors abandonnées au profit d'analyses prédictives permettant de repérer les écarts avant même leur avènement. L'auditeur interne doit donc pouvoir mobiliser ces nouveaux outils dans le cadre de sa fonction. Pour cela, et conformément à la norme d'exercice professionnelle 1230, « les auditeurs internes doivent améliorer leurs connaissances, leurs savoir-faire et autres compétences par une formation professionnelle continue ».

Figure 8 : utilisation de l'analyse de données durant les audits internes



Source : 2017 North american Pulse of internal audit, The Institute of Internal auditors.

[16] 2018 North American Pulse of Internal Audit, The Institute of Internal auditors.

2.2.2.2. Gestion du cyber-risque : audit interne et autres acteurs clés

Dans la dernière étude Risk In focus 2021 menée par l'ECIIA (European Confederation of Institutes of Internal Auditing) auprès de professionnels de l'audit interne, près de 79 % des responsables d'audit interne interrogés considèrent les cyber-risques comme étant le type de risque le plus important auxquels ils doivent faire face. Face à cette crainte partagée au sein du secteur, l'auditeur interne doit jouer un rôle dans la mitigation du risque en collaboration avec d'autres acteurs clés du processus.

En effet, la maîtrise du cyber-risque repose sur un découpage clair des 3 lignes de maîtrise ainsi que sur la collaboration de ces acteurs. La 1re ligne de maîtrise concerne les actions et dispositifs véritablement mis en place au niveau opérationnel afin de lutter contre les menaces de cyberattaques. La 2de ligne de maîtrise est constituée des fonctions de supervision des risques, de contrôle et de conformité ainsi que du responsable de la sécurité des systèmes d'information en charge de s'assurer que les processus et contrôles de la première ligne sont appliqués et respectés. La 3e ligne de maîtrise est représentée par l'audit interne qui doit fournir à la direction générale une assurance objective sur le niveau de maîtrise des risques des processus audités. Le graphique suivant, réalisé à partir des recherches réalisées, permet de visualiser les différentes lignes de maîtrises ainsi que leur rôle dans la gestion des cyber-risques.

Acteurs et rôles dans la gestion des cyber-risques

Instances de gouvernance & comité d'audit

Direction générale

1ère ligne de maîtrise

Service informatique

- Gérer les procédures, les formations et les tests relatifs à la sécurité ;
- Maintenir les configurations de sécurité des appareils, les mises à jour des logiciels et les correctifs de sécurité ;
- Déployer les systèmes de détection d'intrusion et réaliser des tests d'intrusion ;
- Configurer le réseau de façon sécurisée pour gérer et protéger le trafic ;
- Répertorier les actifs informationnels, les appareils technologiques et les logiciels correspondants :
- Mettre en œuvre des programmes de protection des données et de prévention des pertes ainsi qu'une surveillance adaptée ;
- Restreindre les accès par privilège minimal ;
- Chiffrer les données autant que possible ;
- Analyser les vulnérabilités à l'aide de surveillances internes et externes ;
- Recruter et fidéliser des collaborateurs compétents en gestion des systèmes d'informations.

2ème ligne de maîtrise

Responsable de la Sécurité des Systèmes d'information & Contrôle Interne & Risk management & Conformité

- Conception des politiques, formations et tests relatifs à la cybersécurité ;
- Évaluation des cyber-risques ;
- Collecte des informations sur les cybermenaces ;
- • Classification des données et conception d'accès par privilège minimal ;
- Surveillance des incidents, des indicateurs clés de risques et mise en place des correctifs nécessaires ;
- Recrutement et fidélisation de collaborateurs certifiés en gestion des risques SI ;
- Évaluation des relations avec les tiers, les fournisseurs et les prestataires de services ;
- Planification/test de la continuité de l'activité, et participation à des exercices et des tests de reprise après sinistre.

3ème ligne de maîtrise

Audit interne

- Réaliser des évaluations des mesures préventives et de détection liées à la cybersécurité ;
- Évaluer les actifs SI des utilisateurs bénéficiant d'un accès privilégié pour les configurations de sécurité classiques, les sites web posant problèmes, les logiciels malveillants et l'exfiltration de données ;
- Suivre la mise en œuvre des activités de remédiation ;
- Évaluer le cyber-risque global de la structure.

2.3. Secteur sanitaire, audit interne et cybermenace : les spécificités, enjeux et limites au sein du secteur

2.3.1. Le secteur sanitaire, un secteur spécifique

2.3.1.1. Les différents types d'établissements de santé

Le secteur sanitaire regroupe l'ensemble des établissements de santé. Un établissement de santé est une structure définie par un statut légal dont les missions sont régies par le Code de la santé publique. Selon l'article L6111-1 du Code de la santé publique, ce type de structure a pour principal objectif « d'assurer le diagnostic, le suivi et le traitement des malades, des blessés et des femmes enceintes ». Il convient de préciser que tous les établissements prodiguant des soins ne sont pas des établissements de santé. Un cabinet médical par exemple ne rentre pas dans cette définition. Au sein de cette dénomination commune d'établissement de santé, on peut distinguer les établissements publics des établissements privés qui disposent d'activités et de modes de financement différents. Les établissements publics de santé sont des personnes morales de droit public. Sous la forme de structures hospitalières, ils assurent une mission de service public et sont soumis au contrôle de l'État. Ils représentent à eux seuls 61 % du total des lits (utilisés pour représenter la capacité d'hébergement) des établissements de santé en France (figure 9 ci-après). Au sein des structures sanitaires privées, on retrouve deux grandes catégories d'établissement :

- Les établissements à but non lucratif, qui sont des établissements privés participants au service public hospitalier par la réalisation de missions de service public. L'ensemble des bénéfices qu'ils dégagent sont réinvestis dans l'innovation et le développement au profit du patient. Ils représentent près de 14 % de la capacité totale d'accueil des établissements de santé en France ;
- Les établissements à but lucratif sont des sociétés commerciales dispensant des soins médicaux sous la forme d'une clinique privée. Ils représentent près de 24 % de la capacité totale d'hébergement à l'échelle du pays.

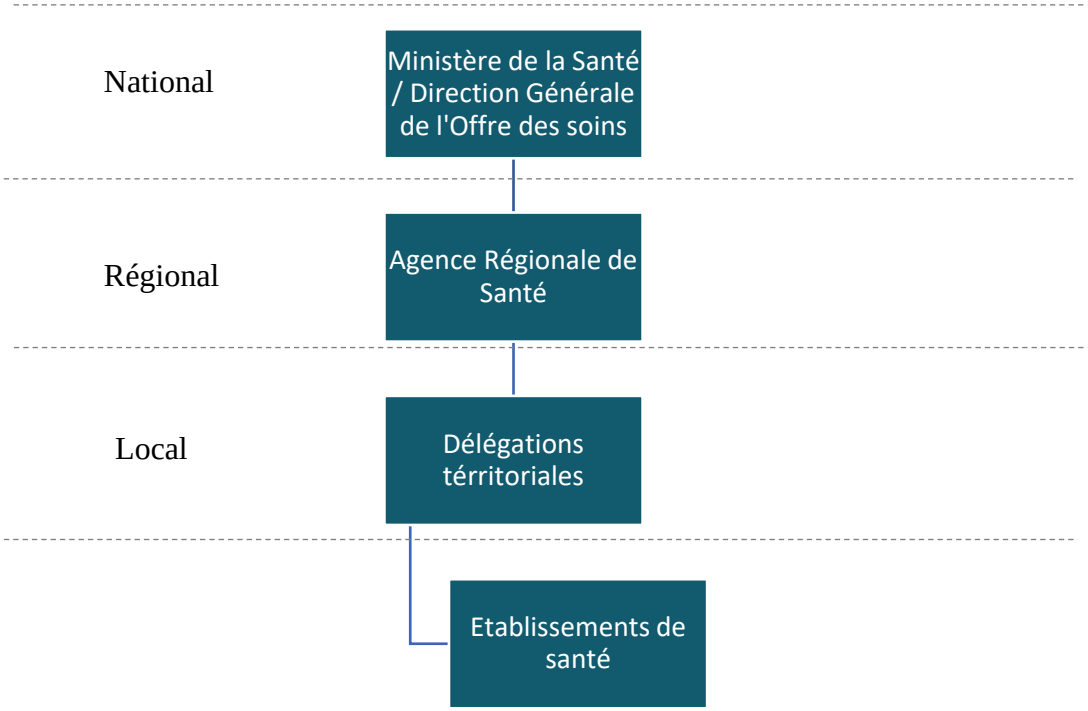
Figure 9 - Établissements de santé au 31 décembre 2018

	Nombre d'entités	Nombre de lits
Secteur public	1 356	243 326
Centres hospitaliers régionaux (CHR/CHU)	1216	234 409
Autres établissements publics	140	8 917
Établissements privés à but non lucratif	681	56 274
Centres de lutte contre le cancer (CLCC)	22	2 772
Autres établissements privés à but non lucratif	659	53 502
Secteur privé (établissements)	999	96 093
Établissements de soins de suite et de réadaptation	348	29 564
Établissements de soins de courte durée[2]	491	52 206
Établissements de lutte contre les maladies mentales	151	13 925
Établissements de soins de longue durée	7	333
Autres établissements privés	9	398
Total	3 036	395 693

Source : tableau de l'économie française édition 2020, la direction de la Recherche, des Études, de l'Évaluation et des Statistiques.

2.3.1.2. La gouvernance des structures sanitaires

Organisation du système de santé en France



Le système français de santé est organisé en 3 principales strates. Au niveau national, le ministère de la Santé et des Solidarités, garant de la cohérence de la prise en charge des patients pilote la stratégie globale. Au niveau régional, les Agences Régionales de Santé (ARS) assurent la coordination de la prévention, des soins et de l'accompagnement. Enfin, au niveau local, les délégations territoriales mettent en œuvre dans les territoires la politique de santé et la politique médico-sociale définie et conduite par l'ARS [17].

Au sein des hôpitaux publics, la gouvernance est séparée entre deux organes depuis la loi Hôpital, Patients, Santé et Territoires (HPST) de 2009. La gestion est entièrement assurée par le directeur de la structure qui a la responsabilité de garantir le bon fonctionnement des services et la pérennité financière. Pour cela, il est aidé par le directoire (ancien Conseil Exécutif). Le conseil de surveillance (ancien conseil d'administration) est quant à lui chargé d'exercer un contrôle permanent sur la gestion et la santé financière de l'établissement et se prononce sur ses orientations stratégiques.

2.3.2. La cybersécurité au sein d'une structure sanitaire : un enjeu majeur

2.3.2.1. Une protection nécessaire des données sensibles et des appareils électroniques…

La révolution numérique a aussi profité au secteur sanitaire. Le développement de la « *e-santé* » visant à mettre au service de la santé les nouvelles technologies est devenu un pan intégrant de la stratégie du système de santé. La prise en charge du patient se veut maintenant numérisée comme le prévoit le programme Ma Santé 2022. L'objectif étant de parvenir à un dossier médical partagé qui serait un carnet de santé numérique propre à chaque citoyen français.

Dans ce contexte, les établissements sanitaires récoltent et stockent de plus en plus de données sensibles afin d'assurer les soins. Ce type de données se caractérise par son aspect particulièrement à risques et son régime de protection renforcée par la Règlementation Générale des Données Personnelles (RGPD). Il

[17] Système de santé, médico-social et social, ministère des Solidarités et de la Santé, disponible sur https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/systeme-de-sante-et-medico-social/article/systeme-de-sante-medico-social-et-social

peut concerner par exemple les antécédents médicaux, les données génétiques, ethniques, ou encore la vie sexuelle du patient. Selon l'entreprise américaine Trustwave spécialisée dans la cybersécurité, une donnée de santé peut être revendue jusqu'à 250$ sur le marché noir contre seulement 5,40$ pour des informations bancaires [18]. Du fait de leur caractère sensible particulièrement profitable pour les cybercriminels, ces données nécessitent un système de protection robuste pour garantir leur sécurité.

Autre composant du système informatique des établissements de santé, les appareils connectés à fin médicale. Les appareils médicaux comme le matériel d'imagerie ou la robotique médicale représentent autant de sources de données et de points d'entrée possibles pour les cybercriminels lorsqu'ils sont connectés au réseau.

En 2021, il y a une attaque majeure par semaine ciblant les hôpitaux contre seulement 27 pour toute l'année 2020 a indiqué le secrétaire d'État à la transition numérique Cédric O interrogé au Sénat. Cette recrudescence d'attaques s'explique principalement par le déploiement du télétravail dans le contexte de la pandémie qui a fragilisé des systèmes d'information déjà sensibles.

2.3.2.2. Mais des ressources néanmoins limitées

Selon Charles Blanc-Rolin, Responsable Sécurité des Systèmes d'information d'un Groupement Hospitalier de Territoire (GHT) et vice-président de l'association pour la sécurité des systèmes d'information de santé, en France, seulement 1 % du budget général d'un hôpital est consacré au domaine numérique en général (en incluant la cybersécurité) contre 5 % à 6 % dans les pays du nord de l'Europe [19]. Cet investissement relativement faible souhaite être renforcé par le gouvernement. La nouvelle stratégie nationale prévoit une enveloppe de 350 millions d'euros dédiés au renforcement de la cybersécurité de ces structures en réponse à l'augmentation des cyberattaques. Ce manque de moyens financiers a pour conséquence de forcer les équipes informatiques à rester en sous-effectif et disposer d'un matériel obsolète vulnérable face aux cyberattaques.

[18] 2019 Trustwave Global Security Report.
[19] Interview disponible sur https://www.stormshield.com/fr/actus/covid-cybersecurite-hopitaux-en-premiere-ligne/

2.3.3. Rôle de l'audit interne dans la gestion des cyber-risques au sein d'une structure sanitaire

2.3.3.1. Établissements de santé et audits

La gestion des risques est au cœur de la stratégie des établissements de santé qui sont de plus en plus incités à identifier, évaluer et prévenir les risques auxquels ils sont confrontés dans la réalisation de leurs activités. L'article L. 6111-2 du Code de la santé publique indique que « les établissements de santé élaborent et mettent en œuvre une politique d'amélioration continue de la qualité et de la sécurité des soins et une gestion des risques visant à prévenir et traiter les événements indésirables liés à leurs activités ». Pour assurer une maîtrise des risques convenable, plusieurs acteurs interviennent pour évaluer le dispositif mis en place par l'établissement de santé. L'Inspection Générale des Affaires sociales (IGAS), en charge du contrôle du secteur, assure les missions « d'audit interne au sein des ministères sociaux et des structures rattachées, afin d'évaluer l'efficacité des dispositifs de maîtrise des risques de ces organismes » [20]. Les services qualité réalisent des audits en interne qui s'inscrivent dans la démarche qualité de l'établissement. La Haute Autorité de Santé évalue l'ensemble des établissements de santé afin d'apprécier la qualité et la sécurité des soins prodigués. Certains établissements de santé disposent de leur propre service d'audit interne, mais aucune obligation légale n'existe, contrairement à d'autres pays comme les États-Unis. Le tableau suivant réalisé à partir des éléments de recherche permet d'identifier les différents types d'audit que peuvent connaitre les établissements sanitaires et leurs principales modalités.

Etablissements de santé et types d'audit

	Commanditaire	Caractère	Opérateur	Périmètre	Référentiel
Audit interne	Structure	Facultatif	Service interne	Limité	Ad hoc
Audit qualité					ISO
Visite d'accréditation	Autorité	Obligatoire	Autorité	Exhaustif	Référentiel d'accréditation
Inspection					Textes législatifs et réglementaires

[20] Ministère des Solidarités et des Santés, disponible sur https://solidarites-sante.gouv.fr/ministere/organisation/organisation-des-directions-et-services/article/inspection-generale-des-affaires-sociales-igas

2.3.3.2. L'audit interne : un acteur clé dans la gestion des cyber-risques

Plus que dans les autres secteurs, les établissements de santé sont particulièrement sensibles aux cyber-risques. La gestion de ce risque n'est pas limitée au directeur des systèmes d'information de la structure. La question doit être envisagée de façon globale, les conséquences n'étant pas seulement techniques, mais aussi opérationnelles. L'audit interne a un rôle essentiel à y jouer. Missionné par le directeur général et le conseil de surveillance, l'audit interne doit apporter à la gouvernance de l'entreprise l'assurance d'un pilotage effectif et pérenne de la cybersécurité, et notamment s'assurer que le pilote du processus bénéficie bien de moyens proportionnés, et de la collaboration des acteurs clés pour maîtriser les risques. Pour cela, il évalue la réalité et l'efficacité des actions engagées au regard des risques afférents à l'aide du directeur des SI et du Responsable sécurité des SI s'il existe. Il va ensuite faire remonter les informations aux organes de directions de manière compréhensible en vulgarisant les termes techniques. Pour assurer ce type de mission, les auditeurs doivent avoir une bonne compréhension des enjeux derrière la cybersécurité et/ou envisager l'intervention d'experts dans ce domaine en fonction du niveau d'assurance souhaité.

2.4. Enquête professionnelle auprès des responsables des systèmes d'information hospitaliers

Afin de disposer d'une vision « terrain », une enquête a été réalisée auprès de responsables des systèmes d'information opérant au sein de centres hospitaliers. Plus de 70 managers ont été contactés, 8 d'entre eux ont accepté de répondre à l'enquête. Ce taux de réponse assez faible (environ 11 %) s'explique principalement par le fait que la cybersécurité des hôpitaux est un sujet particulièrement sensible et que communiquer dessus peut s'avérer dangereux. Certains responsables interrogées ont affirmé qu'ils ne répondaient à aucune question sur la cybersécurité relative à leur structure.

Pour garantir la confidentialité des données, les noms des établissements et des personnes qui ont répondu ne seront pas inclus dans les résultats de l'enquête. Ils seront néanmoins présentés lors de la soutenance pour garantir l'intégrité des données récoltées.

Parmi les huit personnes qui ont répondu, sept occupent le poste de directeur des systèmes d'information (88 %) et une personne est responsable de la sécurité des systèmes d'information (12 %). Ils opèrent tous au sein de centres hospitaliers différents. L'étude a permis de récolter les résultats suivants auprès des responsables informatiques interrogés :

88 % estiment qu'ils ne disposent pas des moyens nécessaires pour assurer la cybersécurité de leur structure ;

100 % estiment que le personnel soignant n'est pas assez sensibilisé aux pratiques élémentaires de sécurité informatique ;

75 % estiment que la cybersécurité n'est pas une priorité pour la gouvernance de leur structure ;

88 % ont réalisé un travail d'évaluation des principaux cyber-risques auxquels est confrontée leur organisation ;

37 % ont déjà subi une cyberattaque majeure au sein de leur structure.

Ces résultats nous permettent d'affirmer que la cybersécurité est une préoccupation majeure pour les responsables informatiques des établissements de santé.

Le détail des réponses est disponible en **annexe 1.**

3. Partie II – Guide d'audit interne de la cybersécurité appliqué à une structure sanitaire

3.1. Présentation de la structure auditée

3.1.1. Avant-propos

Afin de pouvoir analyser toutes les phases qui constituent un audit interne de la cybersécurité d'une structure sanitaire, une mission d'audit va être simulée sur **une structure totalement fictive**. L'ensemble des données et des informations qui concernent cet établissement **ont été entièrement créées** afin de pouvoir réaliser un audit le plus réaliste possible.
Cette partie sera consacrée à la réalisation et à l'analyse du déroulement d'une mission d'audit interne de la cybersécurité au sein d'un établissement de santé. Les documents clés (lettre de mission, référentiel de risque, rapport…) seront entièrement disponibles en annexe. Cette partie se concentrera sur les **principaux éléments clés** de ces documents. Pour une vision exhaustive, il conviendra de se reporter aux annexes.

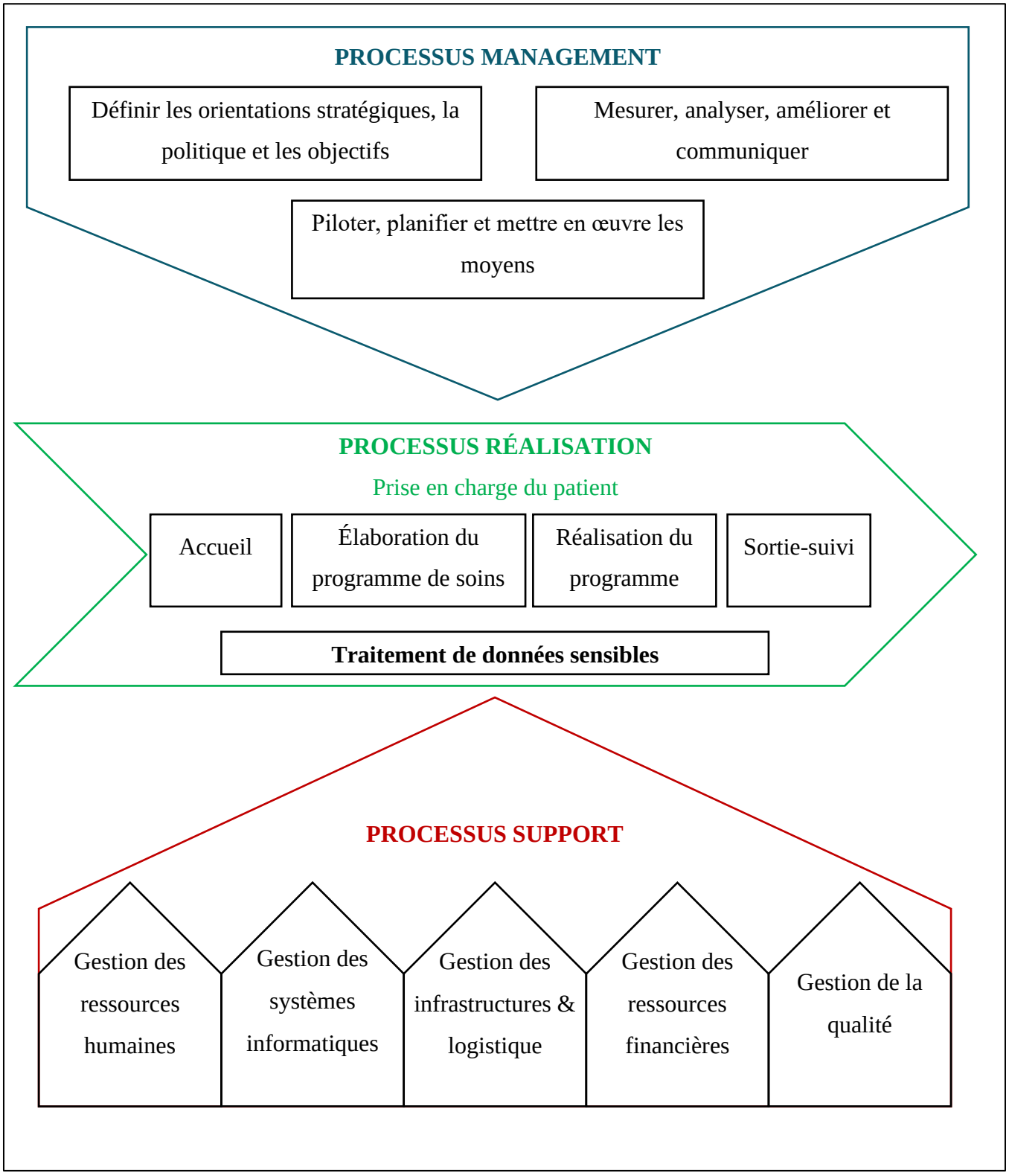
3.1.2. Contexte de la mission d'audit

L'hôpital *Curae* (soin en latin) est un établissement public de santé de proximité situé dans une petite ville en France. De taille modeste, il prend en charge 15 000 patients chaque année (file active). Il dispose de 350 lits et emploie environ 500 salariés dont 15 % font partie des fonctions supports. Il est constitué d'un pôle de médecine générale et d'un pôle de chirurgie oncologie, eux-mêmes composés de différents services. Il dispose d'un budget général annuel de 50 millions d'euros dont 2 % sont consacrés à la gestion des systèmes d'information. L'hôpital ne dispose pas d'un collaborateur entièrement dédié à la cybersécurité du fait de sa taille, c'est donc le directeur des systèmes d'information qui porte ce sujet.
Le nouveau directeur général, qui vient de prendre son poste cette année, reçoit régulièrement des informations de l'ANSSI sur des nouvelles attaques menées contre des hôpitaux de la région. Pleinement conscient des enjeux que représente la cybersécurité, il décide de missionner le service d'audit interne afin d'évaluer le niveau de maitrise des cyber-risques et dresser un premier état des lieux.

3.1.2.1. Cartographie des macro-processus

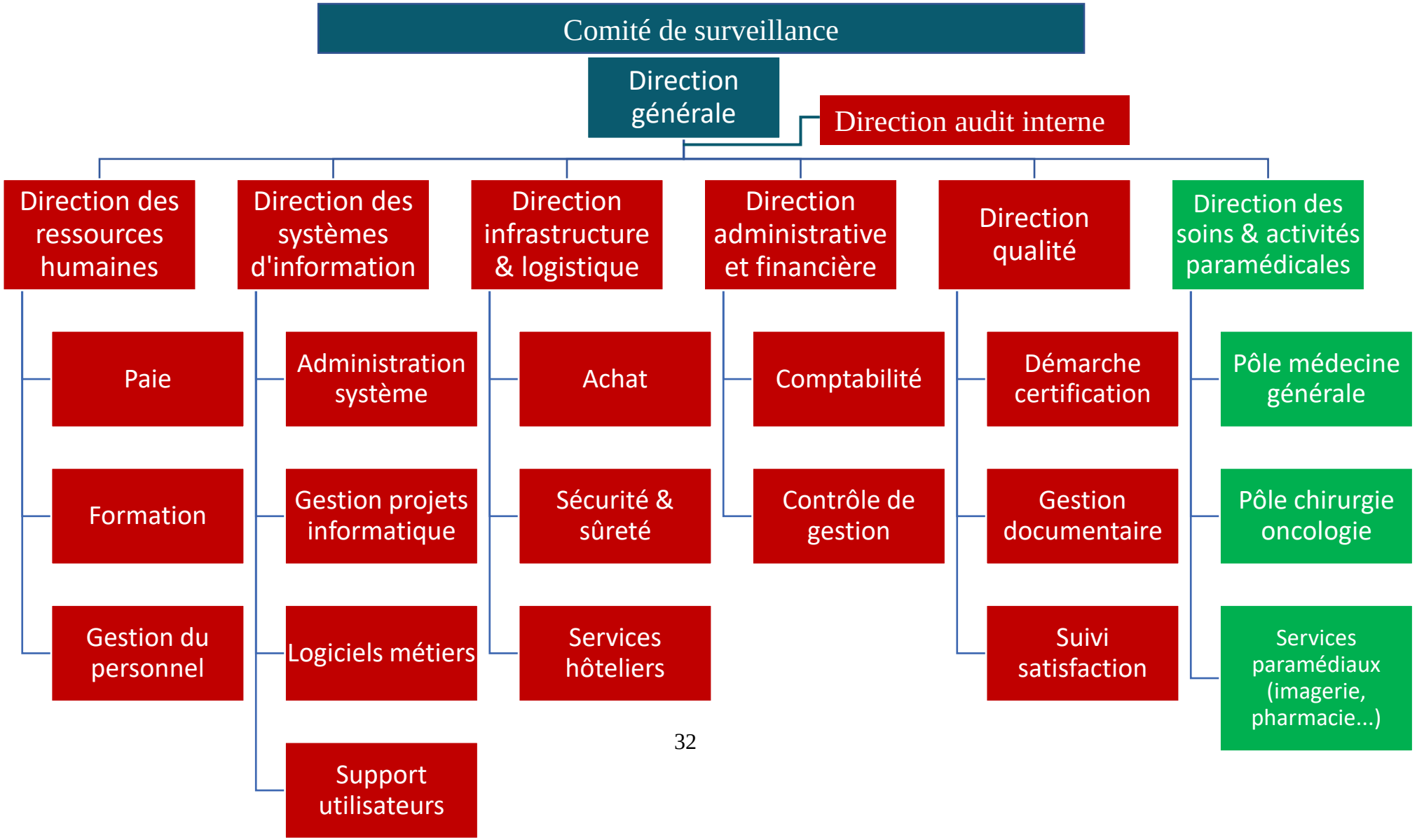
L'approche par processus basée sur la méthode qualité permet le découpage suivant des activités de l'hôpital.

Cartographie simplifiée des processus : prise en charge du patient

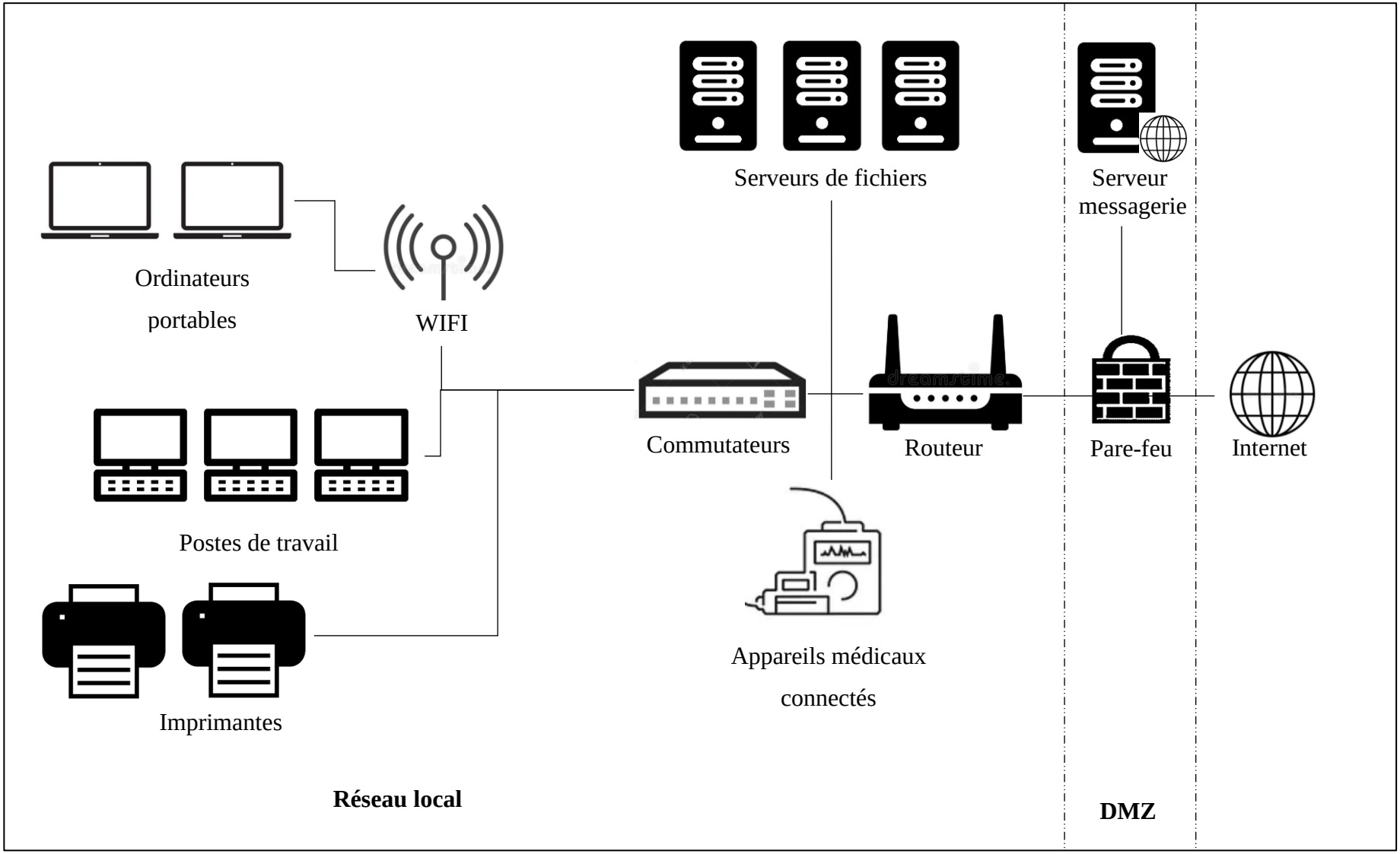


3.1.2.2. Organigramme

L'organigramme suivant reprend l'organisation de la structure avec le découpage par processus. Le bleu représente les responsables du processus management, le vert le processus réalisation et le rouge le processus support.



3.1.2.3. Architecture réseau



Les ordinateurs de la structure sont tous reliés au réseau de manière filaire via des câbles Ethernets ou via wifi. Un antivirus a été installé sur les ordinateurs avant de les mettre à disposition des collaborateurs. L'ensemble du réseau est protégé par un pare-feu dynamique visant à contrôler les communications échangées. Les appareils médicaux connectés sur le réseau transmettent directement leurs données aux serveurs. Les données de l'hôpital sont réparties au sein de 3 serveurs de fichiers :

- Le serveur REVU centralise l'ensemble des données médicales des patients ;
- Le serveur LETO permet la gestion administrative et la facturation des patients ;
- Le serveur TIRI recueille les données issues des appareils médicaux connectés.

La structure dispose de nombreux appareils médicaux connectés. Parmi eux, on retrouve notamment :

- 1 IRM ;
- 1 scanner ;
- 1 gamma caméra ;
- 1 mammographie numérique ;
- 1 robot chirurgical…

3.2. Planification de la mission

3.2.1. Définition des objectifs et du périmètre de la mission

Cette première étape de la mission d'audit, primordiale pour son bon déroulement, sera constituée de 5 sous-étapes qu'il sera nécessaire de compléter en collaboration avec les clients à l'origine de la demande.

A. Détermination des clients

Le client ordonnateur de cette mission est le **directeur général** de la structure. Le **comité de surveillance**, autre organe de direction incontournable au sein de l'hôpital, a validé la tenue de cet audit. Ce sont les deux clients à qui le produit de l'audit est destiné.

B. Détermination de l'évènement déclencheur

Cette mission, qui n'était initialement pas prévue dans le plan d'audit annuel, résulte d'une demande du management à la suite d'une cyberattaque subie par un hôpital de la région. Celui-ci a vu son système informatique totalement bloqué pendant une journée, l'obligeant à fonctionner en mode dégradé.

C. Clarification des attentes des clients

La gouvernance de l'hôpital souhaite disposer d'une évaluation du dispositif de maîtrise des cyber-risques. L'objectif principal de cette mission est d'apprécier la pertinence et l'efficacité des moyens de protection déployés contre les cybercriminels, et de s'assurer de la définition d'une organisation claire et du pilotage du processus.

D. Détermination du périmètre de la mission

Le périmètre de la mission couvrira l'ensemble de l'hôpital et se concentrera naturellement sur le processus support « gestion des systèmes d'information ». Une attention toute particulière sera portée au traitement et à la protection des données issues du processus « prise en charge du patient ». Cette mission sera réalisée par le service d'audit interne conformément aux normes d'exercice professionnel.

E. Déterminer les livrables de la mission

Le principal livrable attendu par les clients est un rapport d'audit complet faisant figurer l'opinion d'audit sur le dispositif de maîtrise des risques.

À l'aide des éléments récupérés auprès des clients, il est maintenant possible de rédiger la lettre de mission qui sera transmise au directeur général pour signature.
Les objectifs de cette mission seront donc les suivants :

- Apprécier l'organisation en place et s'assurer du pilotage du processus de gestion de la cybersécurité ;
- S'assurer de l'efficacité des dispositifs de prévention, détection et protection en matière de cybersécurité.

Le périmètre de la mission couvrira l'ensemble du système d'information de l'hôpital.
La lettre de mission est disponible en **annexe 2**.

3.2.2. **Approche par les risques et construction du référentiel d'audit**

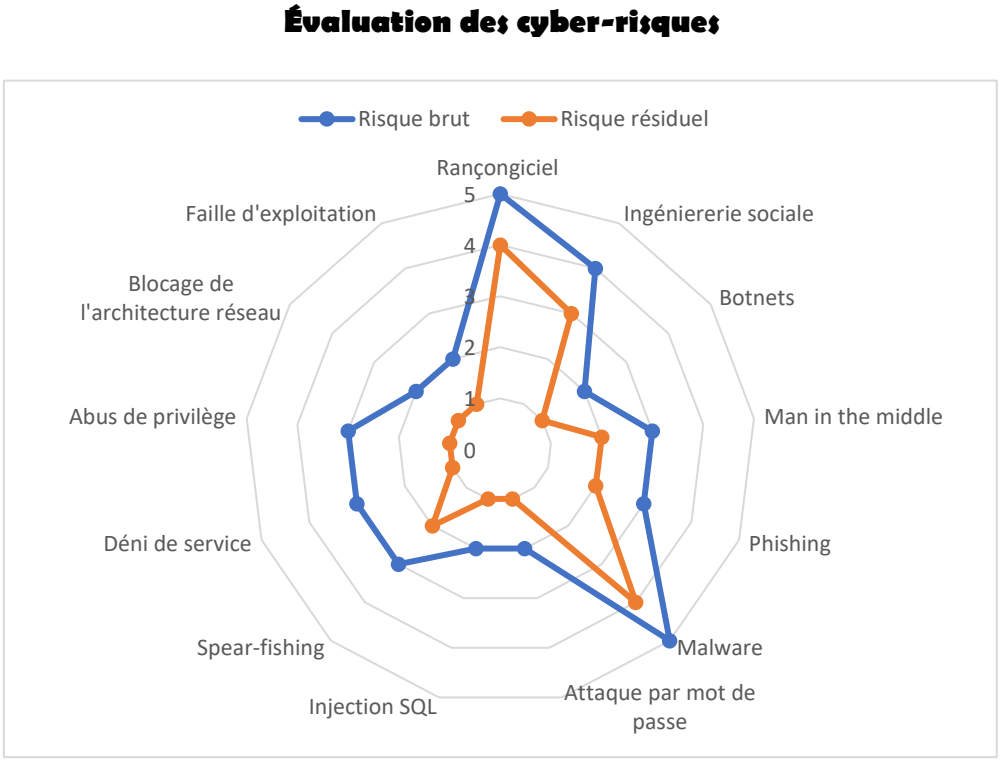
3.2.2.1. Cartographie des risques

À la suite de la réunion d'ouverture réalisée avec le directeur des systèmes d'information afin de lui présenter la mission, l'audit peut débuter. Dans son approche par les risques, l'auditeur interne va se baser sur la cartographie des risques informatiques pour déterminer les axes de ses travaux. Au sein de l'hôpital Curae, ce travail de formalisation n'a pas encore été entrepris. L'audit interne va donc accompagner le directeur des systèmes d'information dans l'élaboration de sa cartographie des cyber-risques (cf. p. 36 & 37).
Un travail de recensement des risques et des moyens de protection déjà en place a ainsi été effectué avec le directeur des SI. Il permet d'identifier trois dangers importants menaçant la cybersécurité de l'hôpital :

- Les rançongiciels visant à bloquer l'accès au réseau de la structure contre le paiement d'une rançon ;
- Une infection par un autre type de malware comme un cheval de Troie ayant pour objectif de récupérer des données confidentielles ;
- L'ingénierie sociale permettant de manipuler un collaborateur via un outil informatique à des fins frauduleuses.

Cartographie des cyber-risques

Objectif	Risque	Probabilité	Gravité	Risque brut	Moyen de protection	Risque résiduel
Fraude	Rançongiciel	4	5	5	Sauvegarde	4
	Ingénierie sociale	4	4	4	Sensibilisation	3
	Botnets	2	3	2	Anti-virus	1
	Man in the middle	3	3	3	Pare-feu	2
	Phishing	5	2	3	Sensibilisation	2
Vol de données médicales	Malware	4	5	5	Sauvegarde	4
	Attaque par mot de passe	1	4	2	Authentification forte	1
	Injection SQL	1	4	2	Serveur sécurisé	1
	Spear-fishing	4	2	3	Sensibilisation	2
Atteinte à l'image	Déni de service	3	3	3	Mises à jour régulières & authentification forte	1
	Abus de privilège	3	4	3		1
Sabotage	Blocage de l'architecture réseau	1	5	2	Organisation clairement définie	1
	Faille d'exploitation	1	5	2	Authentification forte	1



3.2.2.2. Construction du référentiel d'audit

Le référentiel d'audit a pour objectif de recenser les objectifs de chacun des processus et les risques auxquels ils sont exposés ainsi que les contrôles qui devraient permettre de les réduire.

Le référentiel d'audit interne ne devra pas se limiter aux aspects techniques de la cybersécurité. Il devra prendre en compte certains aspects organisationnels complémentaires afin de pouvoir émettre une opinion d'audit pertinente. Le référentiel suivant est composé de 5 grandes parties :

- Implication de la gouvernance et pilotage ;
- Organisation ;
- Prévention ;
- Détection ;
- Protection ;
- Réaction.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
1 – Gouvernance et pilotage					
Implication de la gouvernance	- S'assurer que le comité de surveillance a pris en compte les enjeux liés à la cybersécurité dans la définition de sa stratégie ; - S'assurer qu'il existe un organe de gouvernance dédié à la sécurité numérique.	- Stratégie de l'établissement de santé : - Existence et fréquence des comités ; - Diffusion / publication des comptes rendus.	- La stratégie de l'établissement n'est pas alignée avec les enjeux qu'implique la cybersécurité ; - Le thème de la cybersécurité n'est pas traité au bon niveau hiérarchique.	- Le thème de la cybersécurité est mis à l'ordre du jour des réunions du comité de surveillance au moins une fois par an ; - Un comité cybersécurité impliquant tous les acteurs pertinents de l'établissement se réunit régulièrement afin de piloter la politique de sécurité numérique.	- Vérifier l'existence des comptes-rendus des séances du comité de surveillance ayant eu pour sujet la cybersécurité ; - Contrôler les avis de nomination du comité de cybersécurité ; - Contrôler les comptes-rendus des séances du comité de cybersécurité afin d'en conformer l'existence et sa tenue régulière.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Pilotage du processus	- S'assurer qu'un responsable du processus de gestion de la cybersécurité a été désigné par la gouvernance ; - S'assurer que des objectifs relatifs à ce processus ont été fixés et qu'ils sont alignés avec les attentes de la gouvernance ; - S'assurer qu'il existe des outils de suivi du processus.	- Fiche de poste du responsable cybersécurité ; - Objectifs du processus et attentes de la gouvernance ; - Tableaux de bord de gestion de la cybersécurité.	-Absence de maîtrise du processus ; - Mauvaise gestion et appréciation du processus ; - Décalage entre les objectifs du processus et les attentes de la direction ; - Absence de suivi opérationnel du processus.	- Disposer d'un responsable sécurité SI entièrement dédié à la gestion de la cybersécurité ; - Rattacher hiérarchiquement le RSSI à la direction générale ; - Fixer des objectifs conjointement entre le RSSI et la direction générale ; -Disposer d'outils comme des tableaux de bord pour assurer le suivi opérationnel.	- Obtenir une preuve formelle de la désignation d'un RSSI ; - Vérifier son rattachement hiérarchique à l'aide de l'organigramme de la structure ; - Vérifier la détermination d'objectifs à atteindre à l'aide du compte-rendu du dernier entretien professionnel du RSSI/DSI ainsi que leur suivi opérationnel.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Formalisation d'une politique de sécurité des systèmes d'information	- S'assurer que la structure bénéficie d'une politique formalisée de sécurité des systèmes d'information à jour ; - S'assurer que cette politique est connue par l'ensemble des collaborateurs ; - S'assurer que son contenu est aligné sur les exigences de l'ANSSI.	Politique de sécurité des systèmes d'information claire, pertinente et diffusée à l'ensemble des collaborateurs.	- Non-conformité aux exigences des autorités (certification Haute Autorité de Santé) ; - Méconnaissance de la politique de sécurité par les collaborateurs ; - Non-respect des règles de sécurité internes ; - Absence d'hygiène informatique au sein de la structure.	- Définir la politique de sécurité conjointement entre la direction des SI et le directeur général, et la faire valider par le comité de surveillance ; - Communiquer régulièrement la politique aux collaborateurs et l'inclure dans le livret d'accueil pour les nouveaux arrivants ainsi que sur l'intranet/serveur.	- Vérifier l'existence de la politique de sécurité ainsi que sa transmission via une preuve d'envoi par e-mail et sa dernière date de MAJ ; - Rapprocher son contenu avec les exigences de l'ANSSI ; - Vérifier le compte rendu de la séance de validation de la politique de sécurité par le comité de surveillance.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
2 – Organisation					
Définition de l'organisation	- S'assurer qu'une organisation générale est définie avec des moyens adaptés ; - S'assurer qu'une procédure formalisée définisse les rôles et responsabilités de chacun ; - S'assurer que l'organisation maitrise les risques liés à l'externalisation de ses données.	- Budget alloué à la cybersécurité ; - Procédure gestion de la cybersécurité ; - Contrats des sous-traitants & engagements de confidentialité.	- Confusion des collaborateurs sur leur rôle et leur responsabilité ; - Absence de contrôle de processus. - Absence de contrôle des sous-traitants.	- Dédier 5 à 10 % du budget informatique à la cybersécurité conformément à la stratégie nationale des établissements de santé ; - Formaliser une procédure qui précise les rôles, les responsabilités et les modalités de gestion de la cybersécurité ; - Préciser les responsabilités des sous-traitants en matière de sécurité de l'information au sein d'un accord contractuel.	- Rapprocher le budget informatique global et celui dédié uniquement à la cybersécurité ; - Contrôler l'existence et la pertinence de la procédure « gestion de la cybersécurité » via la réalisation d'entretiens avec les collaborateurs clés ; - Réaliser un entretien avec le directeur des SI. - Revue des accords contractuels des sous-traitants et des clauses précisant leurs responsabilités

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
PROCESSUS MÉTIER 3 – Prévention					
Inventaire des actifs informationnels	S'assurer que les actifs informationnels (dont les dispositifs médicaux connectés) sont identifiés et qu'un inventaire de ces actifs est dressé et tenu à jour.	Inventaire des actifs informationnels.	- Absence de maîtrise du parc des actifs informationnels ; - Perte définitive d'un actif non recensé en cas d'incident.	Procéder régulièrement à un inventaire des actifs informationnels selon des règles définies au sein de la politique de sécurité des SI.	- Revue de la politique de sécurité des SI pour l'identification des règles relatives à l'inventaire ; - Revue de l'inventaire et vérification de son exhaustivité.
Sensibilisation des collaborateurs	S'assurer que l'ensemble des collaborateurs, en particulier le personnel médical amené à traiter des données sensibles, est sensibilisé aux pratiques élémentaires de sécurité informatique.	Programmes de formation et de sensibilisation.	Comportements à risques adoptés par les collaborateurs.	Organiser des actions de formation et de sensibilisation à destination de l'ensemble des salariés et lors de nouveaux recrutements.	- Rapprocher la liste des salariés annoncés comme formés et les listes de présences aux formations prodiguées ; - Envoyer des mails d'hameçonnage aux collaborateurs et vérifier s'ils tombent dans le piège.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Identification des zones critiques	S'assurer que l'établissement a procédé à une analyse des zones critiques de son système d'information.	- Cartographie du réseau informatique ; - Évaluation des cyber-risques.	Vulnérabilité des zones critiques du système d'information face aux attaques.	- Tenue et MAJ régulière d'une cartographie du réseau informatique ; - Hiérarchisation des données traitées et mise en place de moyens de protection différenciés.	- Revue de la cartographie du réseau informatique et de sa dernière date de MAJ ; - Revue de l'évaluation des cyber-risques et des moyens de protection qui y sont relatifs.
Mise à jour des appareils	S'assurer que les appareils connectés au réseau de l'établissement, et en particulier ceux médicaux, ont été mis à jour.	Version des logiciels installés au sein des appareils.	Failles au sein de logiciels obsolètes potentiellement utilisables par les cybercriminels.	Procéder régulièrement à des mises à jour des appareils, logiciels et antivirus utilisés au sein de l'établissement.	Déterminer un échantillon d'appareils connectés et vérifier que le système d'exploitation, les logiciels et les antivirus utilisés sont tous à jour.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Gestion des sauvegardes	S'assurer que l'établissement procède à des sauvegardes sécurisées de ses données.	Rapports de sauvegarde.	Perte définitive des données en cas d'incident.	Procéder à des sauvegardes journalières des données auprès de plusieurs hébergeurs agréés HADS [21] afin de limiter le risque de perte.	Revue des rapports de sauvegarde.
Gestion des accès	S'assurer que les accès des utilisateurs correspondent à leur niveau de besoin.	- Liste des droits d'accès ; - Fiches de poste.	- Mauvais usage, volontaire ou involontaire, des actifs de l'établissement ; - Contrôle total de l'appareil lors d'une cyberattaque en cas de droits accordés trop larges.	Les comptes administrateurs ne doivent être utilisés qu'en cas de nécessité et les droits des utilisateurs limités au strict nécessaire. L'accès aux données médicales ne doit être autorisé qu'au personnel soignant.	- Rapprocher les fiches de poste, la liste des droits d'accès et les logs de connexion au réseau ; - Réaliser un entretien avec l'administrateur des droits d'accès.

[21] Hébergeur Agréé de Données de Santé

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Veille relative aux failles de sécurité	S'assurer qu'une veille relative aux failles de sécurité des logiciels et dispositifs médicaux utilisés est réalisée.	- Cartographie informatique ; - Abonnement CERT.	Utilisation d'outils présentant des failles de sécurité.	Réaliser une veille documentaire à l'aide du CERT Santé.	- Vérifier que les outils utilisés ne sont pas répertoriés comme vulnérables par le CERT Santé ; - Revue des rapports d'installation des correctifs.
Sécurité des mots de passe	S'assurer que des règles robustes d'élaboration de mots de passe sont imposées pour les identifiants internes.	Règles d'élaboration des mots de passe.	Mot de passe simple qui peut être « cassé » par un cybercriminel pour pouvoir ensuite se connecter sur l'espace du collaborateur.	- Règle de blocage des comptes à l'issue de plusieurs échecs de connexion ; - Définition de règles d'élaboration des mots de passe robustes.	- Revue des règles d'élaboration des mots de passe ; - Revue de la configuration de l'identification aux applications internes.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
4 – Détection					
Détection d'intrusion	S'assurer que des dispositifs de détection d'intrusion sont correctement déployés au sein de l'établissement	- Rapports de test des systèmes de détection d'intrusion - Réalisation d'un test d'intrusion.	Attaque non repérée qui laisserait le champ libre au cybercriminel.	Tester régulièrement l'efficacité des systèmes de détection d'intrusion en procédant à des tests d'intrusion.	Revue du fichier du dispositif de détection d'intrusion et des rapports de test.
Surveillance permanente	- S'assurer qu'une permanence est réalisée au sein du service informatique afin de garantir une réponse rapide en cas de cyberattaque.	Planning du service.	Réponse trop tardive en cas d'incident.	Assurer une permanence avec au moins un collaborateur compétent dans le domaine de la cybersécurité.	- Revue du planning du service informatique ; - Réaliser un entretien avec le directeur des SI.
	Mettre en place un système de monitoring (surveillance en français) réseau.	Rapports de surveillance.	Absence de visibilité sur l'activité courante du réseau et à fortiori des signaux faibles de cyberattaque.	Installer un système de monitoring couplé à une permanence du personnel.	Contrôle du fichier de configuration du système de monitoring ; Revue des rapports de surveillance.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Dispositif d'alerte	S'assurer qu'il existe un dispositif d'alerte garantissant une remontée rapide d'informations fiables	Procédure gestion des incidents.	Perte de temps dans la prise de décision qui peut être prise au mauvais niveau hiérarchique.	Définir une procédure de gestion des incidents qui précise les modalités d'alerte.	Revue de la procédure de gestion des incidents et de sa pertinence via la réalisation d'entretiens avec des collaborateurs.
Sécurité physique	S'assurer qu'il existe un contrôle des accès aux salles serveurs.	Liste des personnes habilitées à entrer dans les salles serveurs.	Accès non autorisé d'intrus à un matériel réservé aux personnes habilitées.	- Définir les personnes autorisées à accéder aux espaces réservés ; - Mettre en place un système de surveillance.	Inspection visuelle des collaborateurs accédant aux espaces réservés et rapprochement avec la liste des personnes habilitées.
5 - Protection					
Protection des appareils informatique	S'assurer que les appareils informatiques sont protégés par des antivirus à jour ainsi que par un pare-feu efficace.	- Rapports de fonctionnement des antivirus ; - Règles de filtrage du pare-feu.	Vulnérabilité du réseau et des appareils informatique face aux cybercriminels.	- Installer un antivirus sur l'ensemble des ordinateurs de l'établissement ; - Disposer d'un pare-feu de nouvelle génération.	- Revue des rapports de fonctionnement des antivirus ; - Revue des règles de filtrage du pare-feu.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Cryptographie des données sensibles	S'assurer que les données médicales traitées au sein de l'établissement sont chiffrées.	- Clés cryptographiques ; - Politique d'utilisation des techniques cryptographiques.	Absence de garantie de la confidentialité, de l'intégrité et de l'authenticité des données.	- Définir une politique d'utilisation des techniques cryptographiques ; - Chiffrer les données transmises par les appareils médicaux connectés.	- Revue de la politique d'utilisation des techniques cryptographiques ; - Contrôle du cryptage d'un échantillon de données médicales.
Segmentation du réseau	S'assurer que le réseau est segmenté en faisant recours à des réseaux physiques / logiques différents.	- Cartographie du réseau informatique ; - Diagramme des flux réseaux ; - Inventaire des actifs informationnels.	Accès libre à l'entièreté du réseau en cas d'intrusion.	- Cloisonner son réseau en se basant sur la logique des processus et en protégeant les passerelles (pare-feu, routeur-filtre) entre les différents domaines ; - Centraliser les données médicales au sein d'un même domaine.	- Réaliser un entretien avec l'administrateur réseau ; - Rapprocher la cartographie du réseau informatique, le diagramme des flux réseaux et l'inventaire des actifs informationnels.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
6 - Réaction					
Réagir face à la cyberattaque	S'assurer que l'établissement a défini un protocole à suivre en cas d'intrusion au sein du réseau interne.	Procédure de gestion des incidents.	Absence de réaction ou réaction inadaptée en cas d'intrusion réussie.	Définir la conduite à tenir au sein d'une procédure en cas d'intrusion.	Revue de la procédure de gestion des incidents.
Assurer la continuité d'activité	S'assurer que l'établissement dispose d'un plan de Continuité d'Activité (PCA) permettant d'assurer la continuité d'activité de la prise en charge médicale en mode dégradé.	Plan de Continuité d'Activité.	Arrêt de la prise en charge médicale en cas de cyberattaque.	Prévoir une équipe de réponse à la crise au sein du PCA qui aura été testé en amont lors de simulation de crise afin d'assurer son efficacité fonctionnelle.	- Revue du PCA ; - Réaliser un entretien avec le directeur des SI afin de s'assurer de la pertinence des modalités de continuité d'activité du PCA.

Composante de contrôle interne	Objectifs de contrôle	Risques		Bonnes pratiques	Techniques d'audit
		Points de contrôle	Impacts		
Garantie des cyber-risques	S'assurer que les cyber-risques sont correctement couverts par une police d'assurance dédiée.	Police d'assurance cyber-risques.	Absence de dédommagement en cas de perte d'un actif informationnel.	Disposer d'une assurance cyber-risques couvrant l'ensemble du périmètre du parc informatique de l'établissement de santé.	- Revue de la police d'assurance et contrôle du niveau de couverture.
Analyse post-incident	S'assurer que les incidents et leurs causes sont analysées à posteriori.	Rapports de synthèse des incidents.	Récurrence de l'incident	Analyser les incidents liés à la sécurité des SI en les quantifiant, les qualifiant et en estimant les coûts associés et leurs impacts.	Revue des rapports de synthèse des incidents.

3.2.2.3. Formalisation du programme de travail

L'élaboration d'un programme de travail va permettre de définir les techniques de test appropriées afin d'obtenir une preuve suffisante, pertinente et fiable au regard des objectifs de la mission. C'est lors de cette étape que le responsable de la mission va évaluer les ressources disponibles en interne et les affecter à la mise en œuvre du programme de travail. Pour les aspects les plus techniques de la mission comme les tests d'intrusion, des compétences spécialisées en informatique seront nécessaires. En cas d'absence de collaborateurs compétents dans ce domaine, le responsable pourra recourir à l'aide d'acteurs extérieurs afin externaliser certains aspects de la mission.
C'est ici le cas pour l'équipe d'audit interne de l'hôpital Curae qui sera assisté par un cabinet spécialisé pour les aspects les plus techniques de la mission.
Le programme de travail est disponible **en annexe 3.**

3.3. Accomplissement de la mission

3.3.1. Phase de contrôle sur site

La phase de contrôle sur site va permettre d'obtenir des preuves sur la capacité des dispositifs de contrôle à maîtriser les risques. Elle consistera à réaliser et documenter les tests d'audit afin d'évaluer leurs résultats et élaborer des conclusions.
Au sein de l'hôpital Curae, la première étape du contrôle sur site sera de rencontrer le responsable de la cybersécurité de l'établissement, ici le directeur des SI. Le compte-rendu de cet entretien est disponible **en annexe 4**. À la suite de cette première rencontre, le reste des tests prévu au sein du programme de travail pourra être réalisé à l'aide de feuilles de travail dédiées. Les différents types de feuilles de travail propres à chaque test ne seront pas ici traités du fait de leur caractère protéiforme. Seul un exemple sera présenté. La feuille de travail relative à l'inventaire du parc informatique de l'hôpital est disponible en **annexe 5.**

3.3.2. Formalisation des observations

Cette étape va consister à formaliser les observations issues des tests réalisés. Pour cela, il sera nécessaire d'analyser en profondeur les écarts entre le référentiel et la situation au sein de la structure afin de pouvoir élaborer les recommandations. Celles-ci doivent s'inscrire dans la logique de moyens disponibles au sein de la structure. Les observations pourront être formalisées au sein de FAR (Feuille d'Audit et de Recommandations, historiquement appelée Feuille de Révélation et d'Analyse de Problème) qui permettra de distinguer le constat (écart repéré), les faits, les causes, les conséquences et les recommandations. Les FAR serviront ensuite de base pour la rédaction du rapport. Au sein de l'hôpital Curae, la réalisation de l'ensemble des tests prévus au sein du programme de travail a permis de déterminer les 3 constats majeurs suivants :

- L'organisation actuelle ne permet pas de disposer des moyens nécessaires pour garantir un niveau de maîtrise satisfaisant des cyber-risques ;
- Les outils utilisés ne permettent pas de garantir une protection efficace contre les cyber-attaques ;
- La protection des données médicales est insuffisante au regard des enjeux qu'elle représente.

Les FAR détaillant ces constats sont respectivement disponibles en **annexe 6,7 et 8.**

3.4. Communication des résultats de la mission

3.4.1. Rédaction du rapport d'audit

À la suite de la réunion de clôture conduite avec le responsable du processus afin de valider les observations retenues, la phase de rédaction du rapport d'audit pourra être lancée. Celui-ci consistera à documenter les résultats définitifs et officiels de la mission d'audit pour leurs diffusions aux clients de la mission. Les résultats devront être présentés de manière synthétique et dans un langage *business* afin de garantir leur bonne compréhension par les destinataires du rapport. Ce document final devra reprendre principalement l'objet de la mission, le périmètre de la mission et ses résultats avec l'opinion d'audit sur le niveau de maîtrise global des cyber-risques.

Dans le cas de l'hôpital Curae, le niveau de maîtrise est estimé comme non acceptable. En effet, la structure présente d'importantes vulnérabilités facilement exploitables par les cybercriminels, une action immédiate doit donc être engagée. La diffusion de ce rapport doit permettre une prise de conscience de la gouvernance qui a la responsabilité de considérer les cyber-risques comme un enjeu majeur dans la définition de sa stratégie.
Le rapport d'audit est disponible en **annexe 9**.

3.4.2. Suivi des actions de progrès

Une fois le rapport livré à l'ordonnateur de la mission, l'audit interne devra suivre la mise en place des recommandations émises. Celles-ci représentent la principale plus-value de l'audit réalisé. Les fonctions métiers auront la responsabilité des mettre en place les recommandations au niveau opérationnel. Pour cela, des réunions régulières entre la fonction d'audit interne et les responsables de la mise en œuvre des recommandations devront être organisées.
Au sein de l'hôpital Curae, la lecture du rapport a permis à la gouvernance de prendre conscience des enjeux que représente la cybersécurité. Les recommandations émises sont toutes jugées pertinentes, le directeur général demande au manager du service d'audit interne de l'informer régulièrement sur l'avancée de leur mise en œuvre. Dans ce cadre, le manager décide de créer un tableau dédié au suivi des recommandations qui lui servira de base pour ses échanges avec la direction sur ce sujet.
Le tableau de suivi des recommandations est disponible **en annexe 10.**

4. Conclusion générale

La fonction d'audit interne, autrefois limitée au domaine comptable, a su évoluer pour devenir une véritable fonction de conseil stratégique au service de la gouvernance des organisations. Aujourd'hui devenu un acteur clé dans la gestion des risques, l'audit interne à un rôle important à jouer dans la mitigation des cyber-risques. Ce phénomène directement lié aux cyberattaques est devenu un enjeu majeur pour l'ensemble des structures. En effet, les conséquences des cyberattaques ne se limitent pas seulement au domaine informatique, mais peuvent mettre en péril la pérennité même de l'organisation. Pour s'en protéger, l'auditeur interne intervient en tant que troisième ligne de défense afin d'évaluer le niveau de maturité du dispositif de maîtrise des cyber-risques et en informer la gouvernance de l'établissement. Celui-ci, par son approche systématique et méthodique, va prodiguer à l'établissement une assurance sur le degré de maîtrise de ses opérations en lui apportant ses conseils pour les améliorer et créer de la valeur ajoutée.

Le secteur de la santé, particulièrement vulnérable aux cyberattaques du fait de ses ressources limitées, représente une cible de choix pour les cybercriminels. Le nombre d'attaques informatiques subies par les établissements de santé a explosé en quelques années. Les cybercriminels, motivés par le gain financier, utilisent des techniques de plus en plus poussées pour contourner la sécurité en place. Les réseaux informatiques des établissements de santé disposent en outre de leurs propres spécificités qui peuvent être exploitées par les cybercriminels. En effet, les données de santé collectées par la structure nécessaire à la prise en charge médicale sont particulièrement convoitées par les cybercriminels qui peuvent les revendre sur le marché noir. De plus, les dispositifs médicaux connectés représentent autant de cibles potentielles lors de cyberattaques. Dans ce contexte, l'auditeur interne se doit d'évaluer le niveau de maturité de la cybersécurité de l'établissement afin d'en informer la gouvernance. Afin de donner une assurance pertinente quant au niveau de maîtrise des cyber-risques, l'auditeur ne devra pas se limiter aux aspects techniques du sujet, mais aussi prendre en compte les aspects organisationnels ainsi que les spécificités du secteur dans son approche.

5. Bibliographie

Guides :

IFACI, *Guide des risques cyber IFACI 2.0,* Août 2020, 66 p.

Agence nationale de la sécurité des systèmes d'information, *Guide d'Hygiène Informatique, « renforcer la sécurité de son système d'information en 42 mesures »,* Version 2.0, Septembre 2017, 72 p.

European Union Agency for Cybersécurity, *Procurement guidelines for cybersecurity in hospitals*, Février 2020, 51 p.

IFACI, *Méthodologie de conduite d'une mission d'audit interne*, 92 p.

Ouvrages :

GHERNOUATI Solange, *Cybersécurité - Analyser les risques, mettre en œuvre les solutions,* Dunod, 6e éd, 2019, 973 p.

MAKHLOUF Anissa & HENNION Romain, *Cybersécurité: Un ouvrage unique pour les manager,* Eyrolles; 1ere édition, 2018, 424 p.

AYALA Luis, *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*, Apress, 2016, 201 p.

Articles :

SARRAZIN Claude, *Cybersécurité : misez sur la prévention !*, Gestion, Numéro 2019/3 (Vol. 44), septembre 2019, p. 78-82.

LETORT Jean-Marie, *Cybersécurité : protection des données et des systèmes d'information critiques*, Revue Défense Nationale, 2015/10 (N°785), p. 89 à 92

AH WILLIAMS Patricia & Woodward Andrew, *Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem*, Medical Devices, N°8, Janvier 2015, p. 305-316.

KIM Dong-Won, CHOI Jin-Young, HAN Keun-Hee, *Medical Device Safety Management Using Cybersecurity Risk Analysis*, IEEE, N°8, juin 2020, p. 115370-115382

Kruse, Clemens Scott and al., *Cybersecurity in healthcare: A systematic review of modern threats and trends*, Technology and Health Care, vol. 25, no. 1, 2017, p. 1-10,

Table des matières

ANNEXE 1 – Enquête « terrain »

Réponses enquête « terrain » (1/4)

8 réponses

Réponses acceptées

Résumé | Question | Individuel

Nom et prénom (votre nom et le nom de votre établissement n'apparaîtront pas dans les résultats présentés de l'étude afin de garantir la confidentialité des données collectées)

8 réponses

[redacted]

Poste occupé

8 réponses

DSI du GHT [redacted]

DSI

dsi

RSSI

Directeur du Système d'Information

dsio et communication

DSI

DSI - GHT [redacted]

Nom de l'établissement de santé

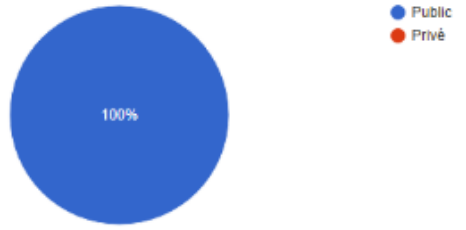
8 réponses

[redacted]

Réponses enquête « terrain » (2/4)

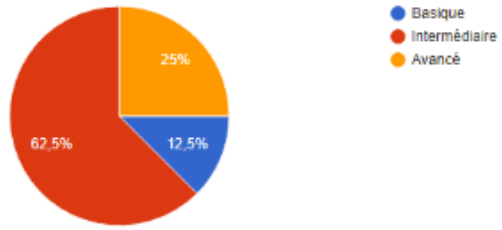
Type d'établissement de santé

8 réponses



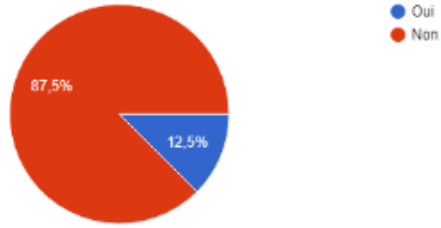
A quel niveau de maturité évaluez-vous la cybersécurité de votre établissement ?

8 réponses



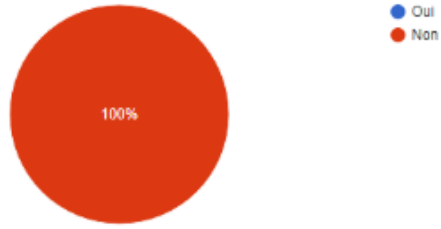
Estimez-vous disposer des moyens nécessaires (humains, financiers...) pour assurer la cybersécurité de votre structure ?

8 réponses



Estimez-vous que le personnel soignant est assez sensibilisé aux bonnes pratiques élémentaires de sécurité informatique ?

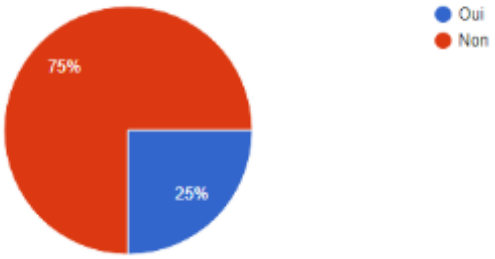
8 réponses



Réponses enquête « terrain » (3/4)

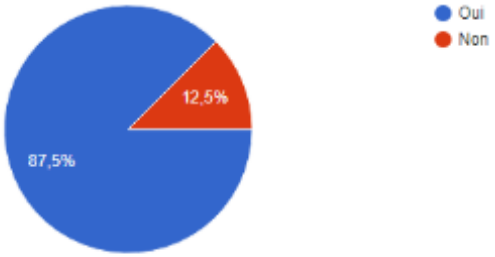
Estimez-vous que la cybersécurité est une priorité pour la gouvernance (direction générale, comités) de votre établissement ?

8 réponses



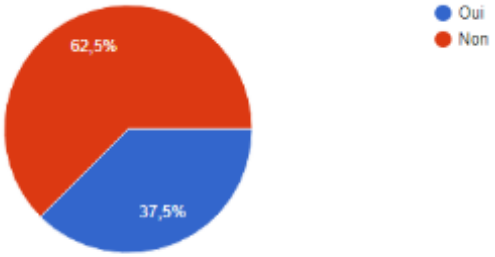
Avez-vous réalisé un travail d'évaluation des principaux cyber-risques auxquels votre établissement est confronté (sous la forme d'une cartographie des risques par exemple) ?

8 réponses



Votre structure a-t-elle déjà subi une cyberattaque majeure ?

8 réponses

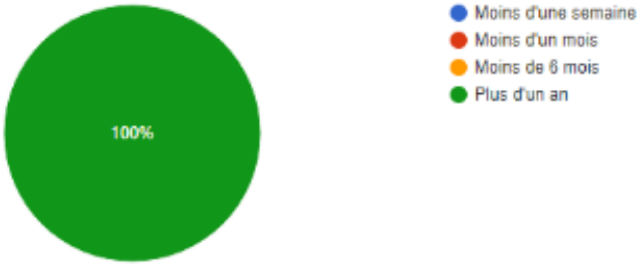


Réponses enquête « terrain » (4/4)

Section 2

De quand date la dernière cyberattaque subie ?

3 réponses

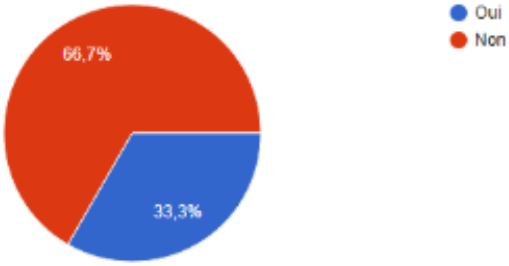


Quel type de cyberattaque était-ce ?

3 réponses

Cette attaque a-t-elle eu un impact sur la continuité d'activité de la prise en charge médicale (fonctionnement en mode dégradé activé par exemple) ?

3 réponses



ANNEXE 2 – Lettre de mission

CURAE

Lettre de mission

Émetteur : Direction Générale **Destinataires** : Direction des SI	**Date** : jeudi 2 septembre 2021
Objet : Audit du dispositif de maîtrise des cyber-risques de l'hôpital Curae	

Conformément à la demande de la gouvernance de l'hôpital, un **audit de la cybersécurité de la structure** va être lancé.

Les objectifs de cette mission sont les suivants :

- Apprécier l'organisation en place et s'assurer du pilotage du processus de gestion de la cybersécurité ;
- S'assurer de l'efficacité des dispositifs de prévention, détection et protection en matière de cybersécurité.

Le périmètre de la mission couvrira l'ensemble du système d'information de l'hôpital.

Cette mission sera réalisée par le **service d'audit interne** de l'hôpital conformément aux normes d'exercice professionnel.

Vous êtes priés d'informer les personnes concernées de la tenue de cette mission.
Les audités prêteront leur concours actif au bon déroulement de la mission et mettront à la disposition des auditeurs les documents, outils et informations nécessaires à la réalisation des objectifs de la mission.

Date de démarrage : 15/06/20XX	**Date prévue de clôture** : 30/08/20XX

X

Le Directeur Général

ANNEXE 3 – Programme de travail

CURAE

Programme de travail

Audit du dispositif de maîtrise des cyber-risques

Objectifs de la mission

Les objectifs de cette mission sont les suivants :

- Apprécier l'organisation en place et s'assurer du pilotage du processus de gestion de la cybersécurité ;
- S'assurer de l'efficacité des dispositifs de prévention, détection et protection en matière de cybersécurité.

Équipe d'audit

L'équipe d'audit interne sera constituée d'un auditeur interne senior jouant le rôle de manager et de deux auditeurs juniors. Pour la réalisation de cette mission, cette équipe sera soutenue par le cabinet XYZ, spécialisé en pentesting, pour la réalisation de certains aspects techniques de la mission.

Estimation du coût de la mission

Au regard du périmètre de la mission, la charge de travail suivante est estimée :

- Manager : 5 à 10 jours/homme ;
- Junior : 10 à 15 jours/homme.

Le devis du cabinet XYZ estime le coût global de sa prestation à 10 000 €.

Composante de contrôle interne	Techniques d'audit	Temps estimé	Responsable [22]	Référence de la feuille de travail
Implication de la gouvernance	- Vérifier l'existence des comptes-rendus des séances du comité de surveillance ayant eu pour sujet la cybersécurité ; - Contrôler les avis de nomination du comité de cybersécurité ; - Contrôler les comptes-rendus des séances du comité de cybersécurité afin d'en conformer l'existence et sa tenue régulière.	½ journée	AS	
Pilotage du processus	- Obtenir une preuve formelle de la désignation d'un RSSI ; - Vérifier son rattachement hiérarchique à l'aide de l'organigramme de la structure ; - Vérifier la détermination d'objectifs à atteindre à l'aide du compte-rendu du dernier entretien professionnel du RSSI/DSI ainsi que leur suivi opérationnel.	½ journée		
Formalisation d'une politique de sécurité des systèmes d'information	- Vérifier l'existence de la politique de sécurité ainsi que sa transmission via une preuve d'envoi par e-mail et sa dernière date de MAJ ; - Rapprocher son contenu avec les exigences de l'ANSSI ; - Vérifier le compte rendu de la séance de validation de la politique de sécurité par le comité de surveillance.	1 journée		

[22] AS = Auditeur Senior, AJ = Auditeur Junior.

Composante de contrôle interne	Techniques d'audit	Temps estimé	Responsable [22]	Référence de la feuille de travail
Définition de l'organisation	- Rapprocher le budget informatique global et celui dédié uniquement à la cybersécurité ; - Contrôler l'existence et la pertinence de la procédure « gestion de la cybersécurité » via la réalisation d'entretiens avec les collaborateurs clés ; - Réaliser un entretien avec le directeur des SI. - Revue des accords contractuels des sous-traitants et des clauses précisant leurs responsabilités	2 journées	AS	
Inventaire des actifs informationnels	- Revue de la politique de sécurité des SI pour l'identification des règles relatives à l'inventaire ; - Revue de l'inventaire et vérification de son exhaustivité.	3 journées	AJ	
Sensibilisation des collaborateurs	- Rapprocher la liste des salariés annoncés comme formés et les listes de présences aux formations prodiguées ; - Envoyer des e-mails d'hameçonnage aux collaborateurs et vérifier s'ils tombent dans le piège.	1 journée	AJ	
Identification des zones critiques	- Revue de la cartographie du réseau informatique et de sa dernière date de MAJ ; - Revue de l'évaluation des cyber-risques et des moyens de protection qui y sont relatifs.	½ journée	AJ	

Composante de contrôle interne	Techniques d'audit	Temps estimé	Responsable [22]	Référence de la feuille de travail
Mise à jour des appareils	Déterminer un échantillon d'appareils connectés et vérifier que le système d'exploitation, les logiciels et les antivirus utilisés sont tous à jour.	1 journée	AJ	
Gestion des sauvegardes	Revue des rapports de sauvegarde.	½ journée	XYZ	
Gestion des accès	- Rapprocher les fiches de poste, la liste des droits d'accès et les logs de connexion au réseau ; - Réaliser un entretien avec l'administrateur des droits d'accès.	½ journée	AJ	
Détection d'intrusion	Revue du fichier du dispositif de détection d'intrusion et des rapports de test. Réalisation d'un test d'intrusion.	3 journées	XYZ	
Surveillance permanente	- Revue du planning du service informatique ; - Réaliser un entretien avec le directeur des SI.	½ journée	AJ	
	- Contrôle du fichier de configuration du système de monitoring ; - Revue des rapports de surveillance.	2 journées	XYZ	
Dispositif d'alerte	Revue de la procédure de gestion des incidents et de sa pertinence via la réalisation d'entretiens avec des collaborateurs.	1 journée	AJ	

Composante de contrôle interne	Techniques d'audit	Temps estimé	Responsable [22]	Référence de la feuille de travail
Protection des appareils informatique	- Revue des rapports de fonctionnement des antivirus ; - Revue des règles de filtrage du pare-feu.	½ journée	XYZ	
Cryptographie des données sensibles	- Revue de la politique d'utilisation des techniques cryptographiques ; - Contrôle du cryptage d'un échantillon de données médicales.	½ journée	XYZ	
Segmentation du réseau	- Réaliser un entretien avec l'administrateur réseau ; - Rapprocher la cartographie du réseau informatique, le diagramme des flux réseaux et l'inventaire des actifs informationnels.	½ journée	AJ	
Réagir face à la cyberattaque	Revue de la procédure de gestion des incidents.	2 journées	AJ	
Assurer la continuité d'activité	- Revue du PCA ; - Réaliser un entretien avec le directeur des SI afin de s'assurer de la pertinence des modalités de continuité d'activité du PCA.			
Garantie des cyber-risques	- Revue de la police d'assurance et contrôle du niveau de couverture.			

ANNEXE 4 – Compte-rendu entretien DSI

CURAE

Compte-rendu entretien

Personne rencontrée(s) et fonction(s) : Martin Dupont, Directeur des SI

Date de l'entretien : 20/06/20XX

Auditeurs : John Doe, Auditeur interne senior

En introduction

- Présentations réciproques
- Rappels des objectifs de la mission d'audit
- Présentation du déroulé de l'entretien

Présentation générale de la direction rencontrée

- **Pourriez-vous me décrire vos principales missions ?**

En tant que directeur des systèmes d'informations de l'établissement Curae, j'ai la responsabilité de définir, construire et maintenir le système d'information hospitalier en lien avec la stratégie de l'organisation et le schéma directeur du système d'information. Outre l'aspect technique de mon métier, j'assure la gestion des moyens confiés, tant humains que financiers, dans l'objectif de garantir un service de qualité. Je suis garant de la sécurité des données traitées au sein de l'hôpital.

- **Pourriez-vous me décrire l'organisation de votre direction ?**

Je supervise une équipe de 10 salariés répartis au sein de 4 services différents :

- L'infrastructure technique en charge de la gestion du réseau et des systèmes et bases de données ;
- La gestion de projets informatiques en charge de l'assistance au déploiement de projets de systèmes d'information ;

- Le service « logiciels métiers » en charge des applications métiers ;
- Le support utilisateur en charge de l'assistance aux utilisateurs.

Description du processus audité

- **Qui pilote la gestion de la cybersécurité au sein de l'établissement ?**

Nous ne disposons pas d'un responsable de la sécurité des systèmes d'information du fait de la petite taille de la structure. Je pilote moi-même la gestion de la cybersécurité au sein de l'établissement.

- **Avez-vous formalisé une politique de sécurité des systèmes d'information ?**

Nous avons en effet défini une politique de sécurité des systèmes d'information. Ce document reste cependant connu des collaborateurs, nous ne l'avons diffusé qu'aux responsables de service.

- **Quels sont les principaux moyens de protection mis en place au sein de Curae vis-à-vis des cybercriminels ?**

Nous procédons à des campagnes de communication régulièrement afin de sensibiliser nos collaborateurs à cette thématique. Le facteur humain est selon moi le plus grand risque dans une structure où la cybersécurité est un enjeu majeur. Nous n'avons pas de budget prévu pour des sessions de formation, seuls des e-mails sont envoyés. Tous nos ordinateurs disposent d'un antivirus programmé pour se mettre à jour automatiquement. Notre pare-feu dynamique est paramétré de manière que seules les connexions réseau légitimes soient autorisées. Nous procédons à des sauvegardes de type miroir de façon journalière. L'ensemble des données médicales est centralisé au sein d'un seul serveur protégé par une authentification forte dont je suis le seul à avoir l'accès administrateur.

- **Avez-vous déjà subi une cyberattaque majeure ?**

Nous n'avons jusqu'ici pas subi de cyberattaque majeure. Un incident lié à un hameçonnage ciblé a eu lieu récemment, mais nous avons su réagir rapidement pour bloquer l'accès des identifiants volés.

- **À quel niveau de maturité évaluez-vous la cybersécurité de l'établissement ?**

Je pense que nous sommes encore sur un niveau basique de sécurité. En effet, le sujet n'est pas une priorité pour la gouvernance et cela se fait ressentir dans les budgets accordés au service informatique. Les moyens que j'ai à ma disposition ne me permettent malheureusement pas de protéger la structure de la manière dont elle le nécessite.

- **Disposez-vous d'outils dédiés au suivi de la cybersécurité ?**

Nous ne disposons pas d'outils de suivi dédiés à la cybersécurité étant donné que nous n'avons quasiment pas d'incidents.

- **Quels sont selon vous les principaux cyber-risques de l'établissement ?**

Les principaux cyber-risques auxquels est exposé Curae sont selon moi le manque d'hygiène informatique des collaborateurs et les vulnérabilités liées aux appareils médicaux connectés. Le personnel soignant qui traite quotidiennement des données sensibles ne maitrise pas les pratiques élémentaires de sécurité informatique. Quant aux appareils médicaux connectés, bien qu'ils représentent une véritable avancée pour le domaine des soins, ils augmentent la surface sur laquelle nous pouvons potentiellement être attaquée.

- **L'établissement est-il assuré contre les cyber-risques ?**

Le parc informatique est couvert par une assurance tous risques informatiques contre les dommages matériels, mais nous ne disposons pas d'une police d'assurance dédiée aux cyber-risques.

- **Avez-vous défini des modalités de gestion de la crise afin de permettre la continuité d'activité ?**

Les modalités de continuité d'activité sont précisées au sein du Plan de Continuité d'Activité de la structure. En cas d'indisponibilité des systèmes d'information, l'activité médicale est maintenue en mode dégradé.

ANNEXE 5 – Inventaire du parc informatique

Inventaire du parc informatique (extrait)

N° interne	Équipement	N° salle	Fonction	Système d'exploitation	Année achat	Marque	État matériel	Numéro série	Date prévue de remplacement
PC-122	Ordinateur fixe	12	Support	XP PRO	2012		Nécessite remplacement	4E21BKBQ10	2017
PC-134	Ordinateur fixe	24	Médicale	XP PRO	2012		Nécessite remplacement	JCBW036126	2017
PC-145	Ordinateur fixe	14	Support	XP PRO	2014		Utilisable	S486559	2019
PC-147	Ordinateur fixe	15	Médicale	Window 10	2016		Performant	S486569	2021
PC-167	Ordinateur fixe	13	Médicale	Window 10	2016		Performant	CN9AVF301B	2021
PC-168	Ordinateur fixe	12	Médicale	Window 10	2016		Performant	S486570	2021
OP-242	Ordinateur portable	14	Support	Window 10	2017		Performant	O9U3U84	2021
OP-243	Ordinateur portable	15	Support	Window 10	2017		Performant	J9EU282	2021
OP-244	Ordinateur portable	16	Support	Window 10	2017		Performant	NC8UU8U	2021
I-356	Imprimante	34	Support	-	2013		Utilisable	G8738	2018
I-546	Imprimante	12	Support	-	2013		Utilisable	G828Y	2018
I-567	Imprimante	14	Médicale	-	2013		Utilisable	F8238Y	2018
AM-21	Appareil médical - IRM	16	Médicale	-	2011		Utilisable	GVY7Y7	2021
AM-24	Appareil médical – Robot chirurgical	16	Médicale	-	2018		Utilisable	VFVF8776	2025

Nombre d’ordinateurs	90
Nombre d’imprimantes	40
Nombre de serveurs	3
Nombre d’appareils médicaux connectés	56

ANNEXE 6 – Fiche d'Audit et de Recommandations N°1

Fiche d'Audit et de Recommandations N°1

Diagnostic du processus **de gestion de la cybersécurité au sein de Curae**.

Constat :

L'organisation actuelle ne permet pas de disposer des moyens nécessaires pour garantir un niveau de maîtrise satisfaisant des cyber-risques.

Faits :

Les tests et les entretiens réalisés dans le cadre de cet audit ont permis de constater que :

- Les moyens financiers mis à disposition du service informatique ne permettent pas de garantir la cybersécurité de la structure. Le budget informatique ne représente que 1 % du budget total de la structure, dont seulement 15 % sont dédiés à la cybersécurité ;
- Les moyens humains ne correspondent au niveau des besoins en termes de cybersécurité. Il n'existe pas de collaborateur entièrement dédié à la gestion de cette thématique, le directeur des SI assume cette responsabilité en parallèle de ses autres activités ;
- Le sujet de la cybersécurité n'est pas assez porté par la gouvernance, il n'a jamais été à l'ordre du jour du comité de surveillance. Le directeur général n'utilise pas son droit de regard pour s'assurer de la bonne gestion du processus au niveau opérationnel ;
- La structure ne bénéficie pas d'une police d'assurance dédiée aux cyber-risques.

Cause :

- La cybersécurité n'est pas considérée comme un sujet majeur par la gouvernance de l'établissement.

Conséquences :

- Les moyens de protection en place contre les cyberattaques ne sont pas suffisants ;
- La gouvernance ne répond pas à sa responsabilité de protéger les données de son établissement. Les dirigeants peuvent voir leur responsabilité personnelle engagée en cas de négligence avérée ;
- L'hôpital ne sera pas dédommagé en cas de dégâts subis à cause d'une cyberattaque.

Recommandations :

Afin d'assurer la maîtrise de ce processus, il convient de mettre en place les actions suivantes :

- Consacrer 5 à 10 % du budget global de l'établissement au service informatique conformément à la stratégie nationale de Santé, dont 20 % seront dédiés à la cybersécurité ;
- Recruter un responsable de la sécurité des SI qui aura la responsabilité de garantir un niveau suffisant de cybersécurité ;
- Responsabiliser la gouvernance en les sensibilisant aux enjeux que représente la cybersécurité ;
- Prévoir des réunions régulières entre le responsable de la sécurité des SI et la gouvernance afin qu'il ait une vision opérationnelle sur la maîtrise des cyber-risques ;
- Souscrire à une assurance dédiée afin d'externaliser les cyber-risques.

ANNEXE 7– Fiche d'Audit et de Recommandations N°2

Fiche d'Audit et de Recommandations N°2

Diagnostic du processus **de gestion de la cybersécurité au sein de Curae**.

Constat :

Les outils utilisés ne permettent pas de garantir une protection efficace contre les cyberattaques.

Faits :

Les tests et les entretiens réalisés dans le cadre de cet audit ont permis de constater que :

- Le réseau interne ne dispose pas d'outil de détection d'intrusion ;
- Le pare-feu dynamique utilisé ne permet pas de protéger l'hôpital contre les menaces avancées comme les logiciels malveillants ;
- Le service informatique ne dispose pas d'un outil de monitoring du réseau ;
- Certains appareils informatiques qui sont obsolètes présentent des vulnérabilités de sécurité.

Causes :

- Politique de sécurité axée sur la protection plutôt que la prévention ;
- Absence de renouvellement régulier du parc des actifs informationnels.

Conséquences :

- Le réseau est vulnérable face aux intrusions ;
- Certains appareils informatiques tournent sur des systèmes d'exploitation obsolètes présentant des vulnérabilités exploitables par les cybercriminels.

Recommandations :

Afin d'assurer la maîtrise de ce processus, il convient de mettre en place les actions suivantes :

- Installer des outils de détection d'intrusion ;
- Acquérir un pare-feu de nouvelle génération intégrant une sécurité renforcée contre les menaces avancées ;
- Installer un outil de monitoring du réseau permettant de repérer les signaux faibles des cyberattaques ;
- Renouveler le parc informatique régulièrement.

ANNEXE 8– Fiche d’Audit et de Recommandations N°3

Fiche d'Audit et de Recommandations N°3

Diagnostic du processus **de gestion de la cybersécurité au sein de Curae**.

Constat :

La protection des données médicales est insuffisante au regard des enjeux qu'elle représente.

Faits :

Les tests et les entretiens réalisés dans le cadre de cet audit ont permis de constater que :

- L'imagerie médicale est basée sur un système de *Picture Archiving and Communication system* (PACS, en français : système d'archivage et de transmission d'image) ne bénéficiant d'aucun chiffrement ;
- Le personnel soignant, en première ligne sur le traitement des données médicales, ne dispose pas d'une hygiène informatique correcte. 35 % d'entre eux ont fourni leurs identifiants lors du test d'hameçonnage ciblé ;
- L'environnement d'exécution via lequel transitent les données médicales n'est pas cloisonné ;
- Certains dispositifs médicaux utilisés présentent des vulnérabilités signalées par le CERT Santé.

Causes :

- Imagerie médicale basée sur un système de transmission non sécurisé ;
- Absence de formation dédiée à la cybersécurité à destination du personnel soignant ;
- L'ensemble du réseau informatique n'est pas segmenté ;
- Absence de veille et de contrôle des dispositifs médicaux.

Conséquences :

- Les images médicales sont consultables en cas d'intrusion ;
- Le personnel soignant a des pratiques informatiques à risques du fait de l'absence de connaissance des règles de sécurité de base ;
- Un intrus peut avoir accès au serveur où est centralisé l'ensemble des données médicales ;
- Certains dispositifs médicaux présentent des vulnérabilités vis-à-vis des cyberattaques.

Recommandations :

Afin d'assurer la maîtrise de ce processus, il convient de mettre en place les actions suivantes :

- Mettre en place un système de cryptage des images médicales ;
- Organiser des sessions de formation dédiées au personnel soignant ;
- Segmenter l'ensemble du réseau et cloisonner l'environnement d'exécution des données médicales ;
- Organiser une veille relative aux signalements des dispositifs médicaux.

ANNEXE 9 – Rapport d'audit

Audit interne du dispositif de maîtrise des cyber-risques de l'hôpital Curae

1

Executive summary 01

Contexte et organisation 02

Présentation des constats détaillés 03

2

01 Executive Summary

3

Executive summary
1.1 Objectifs, périmètre et déroulement

Contexte :

- Une mission d'audit interne de la cybersécurité a été demandée par la gouvernance de la structure. La direction générale a missionnée l'équipe d'audit interne pour réaliser cette mission avec l'aide du cabinet XYZ en soutien.

Objectifs de la mission :

- Apprécier l'organisation en place et s'assurer du pilotage du processus de gestion de la cybersécurité ;
- S'assurer de l'efficacité des dispositifs de prévention, détection et protection en matière de cybersécurité.

Périmètre :

- Le périmètre de la mission couvrira l'ensemble du système d'information de l'hôpital.

4

Executive summary
1.1 Objectifs, périmètre et déroulement

Déroulement :

- La mission d'audit s'est déroulée de juin à août 20XX.
- Au sein de l'hôpital Curae, la responsabilité de la sécurité du système d'information est assumé par le directeur des systèmes d'information. Celui-ci a été une véritable ressource clé lors de la réalisation de cette mission
- Afin de mener la mission d'audit, nos travaux ont été organisés de la façon suivante :
  - La réalisation d'entretien avec le directeur des SI et les autres collaborateurs clés ayant un rôle dans la cybersécurité de la structure ;
  - Le recensement des principaux risques auxquels est confronté l'établissement ;
  - La réalisation de tests afin de s'assurer de la maîtrise des cyber-risques.

5

Executive summary
1.2 Points forts

- La réalisation de cet audit a permis d'apprécier **les points forts suivants** :
  - Un niveau de technicité avancé des collaborateurs du service informatique ;
  - Une politique de sécurité des systèmes d'information définie ;
  - Une organisation bien définie au sein du service informatique intégrant une séparation des tâches satisfaisante ;
  - Des modalités de gestion de la crise visant à permettre la continuité d'activité bien définis au sein du Plan de Continuité d'activité ;
  - Des sauvegardes des données réalisées de manière régulière.

6

Executive summary
1.3 Opinion d'audit

- L'Audit Interne considère la maîtrise des activités **de cybersécurité** comme étant d'un niveau **« non acceptable ».**
- Des axes d'amélioration ont été identifiés au regard des faiblesses suivantes :
  - L'organisation actuelle ne permet pas de disposer des moyens nécessaires pour garantir un niveau de maîtrise satisfaisant des cyber-risques ;
  - Les outils utilisés ne permettent pas de garantir une protection efficace contre les cyber-attaques ;
  - La protection des données médicales est insuffisante au regard des enjeux qu'elle représente

L'opinion de l'Audit est définie de la manière suivante :

Satisfaisant	Perfectible	Incomplet	Non acceptable
Les contrôles sont complets et fonctionnent tels que prévus. Les processus audités sont maîtrisés et formalisés, et les objectifs devraient être atteints de manière à la fois efficace et efficiente.	Les contrôles sont dans l'ensemble appropriés et appliqués. Ils procurent une assurance raisonnable de l'atteinte des objectifs. Toutefois, des évolutions sont souhaitables afin d'améliorer l'efficience du processus audité.	Plusieurs faiblesses de contrôle interne ont été observées. L'atteinte des objectifs du processus n'est pas suffisamment garantie. Des actions rapides sont nécessaires pour renforcer l'efficience du processus audité.	Des principes importants de contrôle interne ne sont pas mis en œuvre. Les objectifs du processus ne seront pas atteints. Une action doit être engagée immédiatement.

7

Executive summary
1.3 Opinion d'audit par axes d'analyse

Notre analyse a été développée autour de **six axes** :

Axes	Opinion
1. Gouvernance et pilotage	Non acceptable
2. Organisation	Incomplet
3. Prévention	Non acceptable
4. Détection	Non acceptable
5. Protection	Incomplet
6. Réaction	Incomplet

8

Executive summary
1.4 Tableau des recommandations

Lien Constats	Actions à mener dans le cadre de la recommandation	Priorité	Réponse Direction	Responsable de la mise en œuvre	Echéance
Constat 1	**Recommandation 1** : consacrer 5 à 10% du budget global de l'établissement au service informatique conformément à la stratégie nationale de Santé, dont 20% seront dédiés à la cybersécurité.	1			
	Recommandation 2 : recruter un responsable de la sécurité des SI qui aura la responsabilité de garantir un niveau suffisant de cybersécurité.	1			
	Recommandation 3 : responsabiliser la gouvernance en les sensibilisant aux enjeux que représente la cybersécurité	1			
	Recommandation 4 : prévoir des réunions régulières entre le responsable de la sécurité des SI et la gouvernance afin qu'elle puisse disposer d'une vision opérationnelle sur la maîtrise des cyber-risques.	2			
	Recommandation 5 : Souscrire à une assurance dédiée afin d'externaliser les cyber-risques.	2			

9

Executive summary
1.4 Tableau des recommandations

Lien Constats	Actions à mener dans le cadre de la recommandation	Priorité	Réponse Direction	Responsable de la mise en œuvre	Echéance
Constat 2	**Recommandation 1** : installer des outils de détection d'intrusion.	2			
	Recommandation 2 : acquérir un pare-feu de nouvelle génération intégrant une sécurité renforcée contre les menaces avancée.	1			
	Recommandation 3 : installer un outil de monitoring du réseau permettant de repérer les signaux faibles des cyberattaques.	1			
	Recommandation 4 : renouveler le parc informatique régulièrement.	2			

10

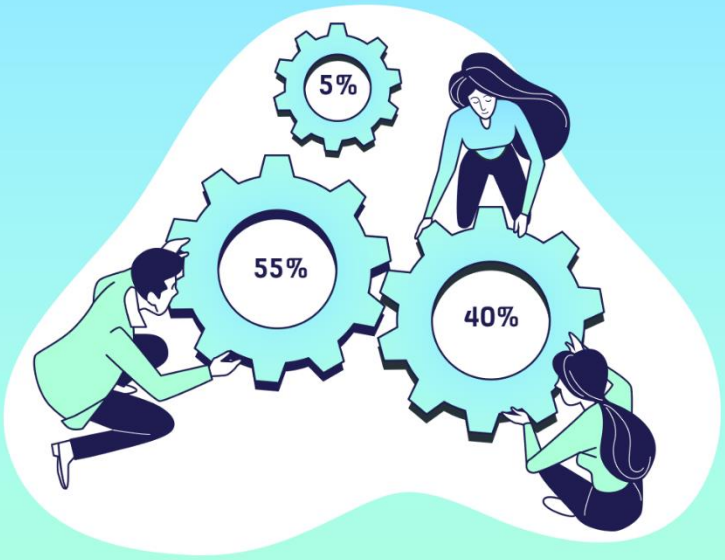
Executive summary
1.4 Tableau des recommandations

Lien Constats	Actions à mener dans le cadre de la recommandation	Priorité	Réponse Direction	Responsable de la mise en œuvre	Echéance
Constat 3	**Recommandation 1** : mettre en place un système de cryptage des images médicales.	2			
	Recommandation 2 : organiser des sessions de formation dédiées au personnel soignant.	1			
	Recommandation 3 : segmenter l'ensemble du réseau et cloisonner l'environnement d'exécution des données médicales.	1			
	Recommandation 4 : organiser une veille relative aux signalements des dispositifs médicaux.	2			

12

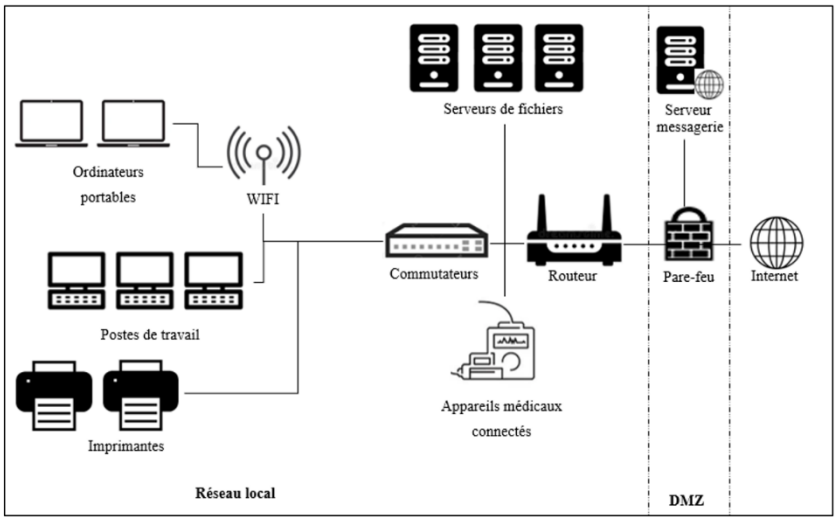
02

Contexte et organisation



13

Contexte et organisation
2.1 Architecture réseau



14

Contexte et organisation
2.1 Cartographie des risques

Objectif	Risque	Probabilité	Gravité	Risque brut	Moyen de protection	Risque résiduel
Fraude	Rançongiciel	4	5	5	Sauvegarde	4
	Ingénierie sociale	4	4	4	Sensibilisation	3
	Botnets	2	3	2	Anti-virus	1
	Man in the middle	3	3	3	Pare-feu	2
	Phishing	5	2	3	Sensibilisation	2
Vol de données médicales	Malware	4	5	5	Sauvegarde	4
	Attaque par mot de passe	1	4	2	Authentification forte	1
	Injection SQL	1	4	2	Serveur sécurisé	1
	Spear-fishing	4	2	3	Sensibilisation	2
Atteinte à l'image	Déni de service	3	3	3	Mises à jour régulières & authentification forte	1
	Abus de privilège	3	4	3		1
Sabotage	Blocage de l'architecture réseau	1	5	2	Organisation clairement définie	1
	Faille d'exploitation	1	5	2	Authentification forte	1

15

03

Présentation des constats détaillés

16

Présentation des constats détaillés
3.1 Constat 1

Fiche d'Audit et de Recommandations N°1

Diagnostic du processus **de gestion de la cybersécurité au sein de Curae**.

Constat :

L'organisation actuelle ne permet pas de disposer des moyens nécessaires pour garantir un niveau de maîtrise satisfaisant des cyber-risques.

Faits :

Les tests et les entretiens réalisés dans le cadre de cet audit ont permis de constater que :

- Les moyens financiers mis à disposition du service informatique ne permettent pas de garantir la cybersécurité de la structure. Le budget informatique ne représente que 1% du budget total de la structure, dont seulement 15% sont dédiés à la cybersécurité ;
- Les moyens humains ne correspondent au niveau des besoins en termes de cybersécurité. Il n'existe pas de collaborateur entièrement dédié à la gestion de cette thématique, le directeur des SI assume cette responsabilité en parallèle de ses autres activités ;
- Le sujet de la cybersécurité n'est pas assez porté par la gouvernance, il n'a jamais été à l'ordre du jour du comité de surveillance. Le directeur général n'utilise pas son droit de regard pour s'assurer de la bonne gestion du processus au niveau opérationnel ;
- La structure ne bénéficie pas d'une police d'assurance dédiée aux cyber-risques.

17

Présentation des constats détaillés
3.1 Constat 1

Cause :

- La cybersécurité n'est pas considérée comme un sujet majeur par la gouvernance de l'établissement.

Conséquences :

- Les moyens de protection en place contre les cyberattaques ne sont pas suffisants ;
- La gouvernance ne répond pas à sa responsabilité de protéger les données de son établissement. Les dirigeants peuvent voir leur responsabilité personnelle engagée en cas de négligence avérée ;
- L'hôpital ne sera pas dédommagé en cas de dégâts subis à cause d'une cyberattaque.

Recommandations :

Afin d'assurer la maîtrise de ce processus, il convient de mettre en place les actions suivantes :

- Consacrer 5 à 10% du budget global de l'établissement au service informatique conformément à la stratégie nationale de Santé, dont 20% seront dédiés à la cybersécurité ;
- Recruter un responsable de la sécurité des SI qui aura la responsabilité de garantir un niveau suffisant de cybersécurité ;
- Responsabiliser la gouvernance en les sensibilisant aux enjeux que représente la cybersécurité ;
- Prévoir des réunions régulières entre le responsable de la sécurité des SI et la gouvernance afin qu'elle puisse disposer d'une vision opérationnelle sur la maîtrise des cyber-risques ;
- Souscrire à une assurance dédiée afin d'externaliser les cyber-risques.

18

Présentation des constats détaillés
3.2 Constat 2

Fiche d'Audit et de Recommandations N°2

Diagnostic du processus **de gestion de la cybersécurité au sein de Curae**.

Constat :

Les outils utilisés ne permettent pas de garantir une protection efficace contre les cyberattaques.

Faits :

Les tests et les entretiens réalisés dans le cadre de cet audit ont permis de constater que :

- Le réseau interne ne dispose pas d'outil de détection d'intrusion ;
- Le pare-feu dynamique utilisé ne permet pas de protéger l'hôpital contre les menaces avancées comme les logiciels malveillants ;
- Le service informatique ne dispose pas d'un outil de monitoring du réseau ;
- Certains appareils informatiques qui sont obsolètes présentent des vulnérabilités de sécurité.

Causes :

- Politique de sécurité axée sur la protection plutôt que la prévention ;
- Absence de renouvellement régulier du parc des actifs informationnels.

19

Présentation des constats détaillés
3.2 Constat 2

Conséquences :

- Le réseau est vulnérable face aux intrusions ;
- Certains appareils informatiques tournent sur des systèmes d'exploitation obsolètes présentant des vulnérabilités exploitables par les cybercriminels.

Recommandations :

Afin d'assurer la maîtrise de ce processus, il convient de mettre en place les actions suivantes :

- Installer des outils de détection d'intrusion ;
- Acquérir un pare-feu de nouvelle génération intégrant une sécurité renforcée contre les menaces avancée ;
- Installer un outil de monitoring du réseau permettant de repérer les signaux faibles des cyberattaques ;
- Renouveler le parc informatique régulièrement.

20

Présentation des constats détaillés
3.3 Constat 3

Fiche d'Audit et de Recommandations N°3

Diagnostic du processus **de gestion de la cybersécurité au sein de Curae**.

Constat :

La protection des données médicales est insuffisante au regard des enjeux qu'elle représente.

Faits :

Les tests et les entretiens réalisés dans le cadre de cet audit ont permis de constater que :

- L'imagerie médicale est basée sur un système de *Picture Archiving and Communication system* (PACS, système d'archivage et de transmission d'image en français) ne bénéficiant d'aucun chiffrement ;
- Le personnel soignant, en première ligne sur le traitement des données médicales, ne dispose pas d'une hygiène informatique correcte. 35% d'entre eux ont fournis leurs identifiants lors du test d'hameçonnage ciblé ;
- L'environnement d'exécution via lequel transitent les données médicales n'est pas cloisonné ;
- Certains dispositifs médicaux utilisés présentent des vulnérabilités signalées par le CERT Santé.

21

Présentation des constats détaillés
3.3 Constat 3

Causes :

- Imagerie médicale basé sur un système de transmission non sécurisé ;
- Absence de formation dédiée à la cybersécurité à destination du personnel soignant ;
- L'ensemble du réseau informatique n'est pas segmenté ;
- Absence de veille et de contrôle des dispositifs médicaux.

Conséquences :

- Les images médicales sont consultables en cas d'intrusion ;
- Le personnel soignant a des pratiques informatiques à risques du fait de l'absence de connaissance des règles de sécurité de base ;
- Un intrus peut avoir accès au serveur où est centralisé l'ensemble des données médicales ;
- Certains dispositifs médicaux présentent des vulnérabilités vis-à-vis des cyberattaques.

22

Présentation des constats détaillés
3.3 Constat 3

Recommandations :

Afin d'assurer la maîtrise de ce processus, il convient de mettre en place les actions suivantes :

- Mettre en place un système de cryptage des images médicales ;
- Organiser des sessions de formation dédiées au personnel soignant ;
- Segmenter l'ensemble du réseau et cloisonner l'environnement d'exécution des données médicales ;
- Organiser une veille relative aux signalements des dispositifs médicaux.

23

Annexe 10 – Tableau de suivi des recommandations

Tableau de suivi des recommandations (1/2)

Intitulé de la mission d'audit interne	Date de remise du rapport	N° reco.	Intitulé de la recommandation	Priorité	En charge de la mise en œuvre	% mises en œuvre	Dernière date MAJ	Commentaires
Audit interne du dispositif de maîtrise des cyber-risques	Août 20XX	1	**Recommandation 1.1** : consacrer 5 à 10 % du budget global de l'établissement au service informatique conformément à la stratégie nationale de Santé, dont 20 % seront dédiés à la cybersécurité.	1	Direction générale			
			Recommandation 1.2 : recruter un responsable de la sécurité des SI qui aura la responsabilité de garantir un niveau suffisant de cybersécurité.	1	Direction générale			
			Recommandation 1.3 : responsabiliser la gouvernance en les sensibilisant aux enjeux que représente la cybersécurité	1	Directeur des SI			
			Recommandation 1.4 : prévoir des réunions régulières entre le responsable de la sécurité des SI et la gouvernance afin qu'il ait une vision opérationnelle sur la maîtrise des cyber-risques.	2	Directeur des SI, directeur général et comité de surveillance			
			Recommandation 1.5 : Souscrire à une assurance dédiée afin d'externaliser les cyber-risques.	2	Directeur général			
		2	**Recommandation 2.1** : installer des outils de détection d'intrusion.	2	Responsable de la sécurité des SI			
			Recommandation 2.2 : acquérir un pare-feu de nouvelle génération intégrant une sécurité renforcée contre les menaces avancées.	1	Responsable de la sécurité des SI			
			Recommandation 2.3 : installer un outil de monitoring du réseau permettant de repérer les signaux faibles des cyberattaques.	1	Responsable de la sécurité des SI			
			Recommandation 2.4 : renouveler le parc informatique régulièrement.	2	Responsable de la sécurité des SI			

Tableau de suivi des recommandations (2/2)

		3	**Recommandation 3.1** : mettre en place un système de cryptage des images médicales.	2	Responsable de la sécurité des SI			
			Recommandation 3.2 : organiser des sessions de formation sur la cybersécurité dédiées au personnel soignant.	1	Direction des ressources humaines			
			Recommandation 3.3 : segmenter l'ensemble du réseau et cloisonner l'environnement d'exécution des données médicales	1	Responsable de la sécurité des SI			
			Recommandation 3.4 : organiser une veille relative aux signalements des dispositifs médicaux.	2	Responsable de la sécurité des SI			