RAPPORT D'ENQUÊTE QUALITATIVE GIS MARSOUIN

CYBERSÉCURITÉ DES ENTREPRISES BRETONNES DE PLUS DE 10 SALARIÉS

JUIN 2025

WWW.MARSOUIN.ORG

Marsouin
© Recherche sur la société numérique et l'innovation

Région Bretagne

Bretagne Développement Innovation

Table des matières

Résumé

Ce rapport présente les résultats d'une enquête qualitative exploratoire menée par le Groupement d'intérêt scientifique (GIS) Marsouin, avec le soutien de la Région Bretagne, sur les perceptions et pratiques des entreprises bretonnes en matière de cybersécurité. L'objectif est de mieux comprendre comment les entreprises de plus de dix salariés se positionnent face à l'augmentation des menaces cyber, dans un contexte de transformation digitale rapide et de renforcement des obligations réglementaires européennes et nationales.

Les systèmes numériques sont aujourd'hui au cœur du fonctionnement des entreprises. Cette dépendance les rend vulnérables à une diversité croissante de menaces : attaques par rançongiciel, exfiltration des données, déni de service, ou encore déstabilisation par des groupes hacktivistes. Les petites et moyennes entreprises (PME) sont particulièrement ciblées, souvent en raison d'une préparation insuffisante. En parallèle, les exigences réglementaires (NIS2, ISO27001, DORA, LOPMJ, etc.,) se renforcent et poussent les entreprises à se mettre en conformité.

L'enquête menée auprès de onze entreprises bretonnes issues de secteurs variés (industrie, numérique, santé, logistique, agriculture, agroalimentaire) met en lumière une diversité de situations, de niveaux de préparation et de maturité en matière de cybersécurité.

L'analyse révèle que la cybersécurité est souvent perçue de manière pragmatique. Pour certaines entreprises, elle constitue un levier stratégique intégré à la gouvernance, notamment dans les services numériques ou très régulés. Ces entreprises ont mis en place une gouvernance dédiée, des certifications (comme ISO27001), des plans de continuité d'activité, et des dispositifs de sensibilisation des collaborateurs.

A l'inverse, d'autres entreprises, notamment les plus petites parmi celles enquêtées et dont l'IT n'est pas le cœur de métier, ont une approche plus minimaliste : elles externalisent la quasi-totalité de leur sécurité numérique à des prestataires. Cette externalisation traduit à la fois un manque de structuration interne, un déficit de compétences en interne et parfois une moindre reconnaissance de la cybersécurité dans la stratégie de l'entreprise. La sécurité numérique est alors traitée comme une fonction isolée, sans vision d'ensemble.

L'enquête fait ressortir plusieurs fragilités partagées par les entreprises interrogées : une dette technique à rattraper, une dépendance accrue aux prestataires externes (externalisation quasi-totale de la cybersécurité dans certaines entreprises, souvent par défaut, multiplication du recours aux prestataires pour toutes les entreprises enquêtées), une structuration de la cybersécurité faible ou absente (absence de structure interne claire pour piloter la sécurité, pas de RSSI, pas de comité dédié, etc.), une pression sectorielle et réglementaire croissante (conformité imposée par des clients ou le secteur, avec peu de marge d'initiative interne), un manque de sensibilisation et de culture cyber en interne (faible implication des collaborateurs, manque de formation et d'appropriation de bonnes pratiques), une préparation encore insuffisante à la gestion d'incident et à la résilience (plans de continuité ou de reprise d'activité peu ou pas formalisés, manque d'exercices de crise), des enjeux émergents liés à l'intelligence artificielle (prise de conscience en cours, mais peu d'intégration des risques liés à l'IA dans les stratégies cyber).

Afin de mieux comprendre les logiques d'appropriation de la cybersécurité, l'étude propose une typologie structurée autour de trois profils d'entreprises :

- Profil 1 - Maturité avancée : Entreprises ayant intégré la cybersécurité dans leur stratégie, avec un pilotage autonome, une gouvernance structurée, et une capacité d'anticipation. La sécurité est ici un facteur de compétitivité et de confiance.
- Profil 2 – Maturité intermédiaire : Entreprises conscientes des enjeux mais encore en transition, souvent stimulées par des pressions externes (clients, audits, réglementation) sans disposer de tous les moyens ou outils pour formaliser une stratégie complète.
- Profil 3 – Maturité faible ou fragmentaire : Entreprises pour lesquelles la cybersécurité reste périphérique, externalisée, peu comprise en interne, et abordée avant tout sous l'angle de la contrainte plutôt que de l'opportunité.

Face à cette diversité de situations, plusieurs pistes d'accompagnement peuvent être envisagées : 1) renforcer la gouvernance interne en incitant à la désignation de référents cybersécurité, à la mise en place de comités, et à l'élaboration des tableaux de bord ; 2) développer la culture cyber à travers des programmes de formation et de sensibilisation adaptés aux réalités métiers ; 3) structurer la résilience en accompagnant les entreprises dans la formalisation et la mise à l'épreuve de plans de continuité d'activité ; 4) cibler des aides publiques selon les profils de maturité afin de soutenir les investissements nécessaires, tout en valorisant les démarches engagées.

Au final, ce rapport montre que la cybersécurité ne peut plus être pensée comme une simple fonction technique ou un coût à maîtriser. Elle conditionne la continuité d'activité, la confiance des partenaires et la compétitivité sur des marchés de plus en plus régulés. Elle devient un enjeu stratégique, transversal et collectif, à intégrer dans les pratiques quotidiennes, la gouvernance et les orientations d'avenir des entreprises. L'approche par la maturité, telle qu'elle ressort des entretiens réalisés, permet non seulement de mieux comprendre les besoins différenciés des entreprises bretonnes, mais aussi d'orienter les politiques publiques ciblées et efficaces.

Rapport sur l'Enquête qualitative sur la cybersécurité des entreprises bretonnes de plus de dix salariés

GIS Marsouin, Juin 2025.

Le Groupement d'Intérêt Scientifique Marsouin remercie ses interlocuteurs (des Dirigeants d'entreprise, des Responsables d'Infrastructure, responsables Sécurité SI, IT Architecture, IT & OTI, Délégué à la protection des données (DPO)) qui nous ont accordé du temps en acceptant de participer à un entretien. Ces temps d'échange, l'intérêt pour le sujet, les compétences professionnelles et la réflexivité de nos interlocuteurs font toute la richesse du matériau de cette enquête qualitative exploratoire dont nous présentons ici les résultats principaux.

Cette enquête a été réalisée par le GIS Marsouin avec un financement de la Région Bretagne.

Introduction

Dans des sociétés où désormais presque toutes les activités humaines dépendent des systèmes technologiques d'information et de communication, les entreprises, comme toute organisation, sont vulnérables aux cyberattaques. De nombreux composants comme des capteurs ou des automates industriels se trouvent désormais aussi connectés et interdépendants, constituant ainsi un « cyberespace » de plus en plus étendu. La captation d'informations, la maîtrise de l'intégrité des données stockées, l'altération des systèmes d'informations d'une entreprise, d'une organisation, l'usurpation d'identité, le détournement de flux financiers ou encore le piratage des messageries peuvent devenir un avantage stratégique déterminant. La cybersécurité des entités essentielles, importantes et critiques (par exemple les réseaux d'énergie, les processus de production industriels, la défense, les systèmes financiers) constitue une problématique majeure, dans un contexte d'enjeu national. Ces nouvelles formes d'affrontement menacent la sécurité des entreprises, pouvant entraîner des pertes financières, du vol de données et pouvant aller jusqu'à porter atteinte à la confiance des clients. Les PME-PMI sont également des victimes potentielles, au même titre que les multinationales. Les sociétés sous-traitantes d'un plus grand groupe peuvent servir de porte d'entrée pour des pirates dès lors qu'elles sont plus facilement accessibles, moins équipées en matière de sécurité, elles permettent d'infecter le système d'information de leurs clients (Arpagian, 2022).

Le domaine de la cybersécurité concerne les usages défensifs et offensifs de ces systèmes d'information (Arpagian, 2022). A la fois menace et ressource, la cybersécurité comporte cette « identité dédoublée » dans la sécurité informatique, comme l'avaient déjà souligné N. Auray et D. Kaminsky (2008). La cybersécurité prend en compte les moyens techniques utilisés pour l'échange de données, mais aussi les « contenus » c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (informatique industrielle, site internet, base de données, communications électroniques, transactions dématérialisées etc.). La cybersécurité porte donc aussi bien sur la protection et l'attaque d'équipements informatiques afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur Internet et les possibilités d'atteinte à la réputation, le vol de données sensibles par exemple. Le champ des menaces possibles est vaste, suivant un principe de « guerre asymétrique » (Arpagian, 2022).

Contexte et questionnement

La quatrième édition du Panorama de la Cybermenace de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) 2024, publié en 2025[1], confirme la tendance de la persistance des cybermenaces avec un maintien à un niveau comparable aux années précédentes du nombre d'attaques, par exemple par rançongiciels dans un « écosystème renforcé afin d'assurer la réponse à ce type d'attaques » ; les PME-TPE-ETI constituant la catégorie d'entité la plus affectée par ces compromissions. Les attaques à but de déstabilisation (par DDoS,

[1] CERTFR-2025-CTI-003, Panorama de la Cybermenace 2024, publié le 11 mars 2025. https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/

défiguration de site Web ou revendication d'exfiltration de données), particulièrement nombreuses au cours de l'année 2024, avaient pour cible de petites installations industrielles, en portant atteinte par exemple à la disponibilité du service visé. Menées par des groupes hacktivistes, elles sont identifiées par l'ANSSI comme ayant un faible niveau de technicité mais une forte capacité médiatique. Le rapport annuel de la Cybercriminalité 2024 (données 2023) souligne un accroissement du champ de la criminalité numérique à travers une diversité des phénomènes cybercriminels recensés, une professionnalisation significative en matière d'appropriation des outils techniques et une industrialisation des processus cybercriminels. Plusieurs hypothèses expliquent cette hausse observée : le développement des usages numériques et donc un accroissement de la surface d'attaque possible, l'amélioration du signalement des infractions ; d'autant qu'une partie significative de la cybercriminalité n'est pas enregistrée dans les données judiciaires. A partir des exemples concrets d'incidents traités, les derniers rapports notifient, d'une part, l'évolution des intentions des acteurs malveillants (espionnage stratégique et industriels, attaques à but lucratif, opérations de déstabilisation), leurs capacités et les opportunités qu'ils ont exploitées pour compromettre des systèmes d'information ; d'autre part, ils relatent les actions de lutte qui sont menées[2].

Les documents disponibles analysés sur le sujet décrivent donc divers aspects de la cybersécurité. Sous l'angle de l'attaque et des usages offensifs, ils rendent compte des menaces croissantes. Sous l'angle de la protection et des usages défensifs des systèmes d'information, ils font part non seulement des évolutions juridiques que sont par exemple les réglementations européennes (le *Cybersecurity Act* ; les Directives NIS, NIS2 ; DORA)[3], ou des évolutions légales[4] (ex. LOPMI et LOPMJ 2023 ; DSA 2024)[5], mais aussi des stratégies de prévention qui sont prévues dans ses réglementations, avec l'essor d'une normalisation de la cybersécurité notamment dans les entreprises où les normes et certifications (ex. ISO/CEI 27032)[6] se développent, ainsi que l'importance de l'information, la sensibilisation et la formation des employés, et le déploiement de plans intégrés (ex. « *privacy by design* » ; plans d'urgence etc.).

Concrètement, la cybersécurité nécessite une approche multidimensionnelle d'adoption de « bonnes pratiques » pour construire un environnement numérique sécurisé. Mais sur le terrain, particulièrement pour les PME-TPE-EPI, l'écart entre ce que l'on sait faire en matière de cybersécurité aujourd'hui – tant du point de vue des outils que des *process* – et les pratiques quotidiennes des entreprises apparaît important. Face à l'augmentation des risques cyber, comment les entreprises se préparent-elles et se protègent-elles ? Quelles sont les normes et les réglementations appliquées pour encadrer leur cybersécurité ? Comment sensibilisent-elles et forment-elles leurs employés pour qu'ils deviennent des acteurs proactifs ?

Une enquête locale exploratoire et qualitative

Depuis 2022, la Région Bretagne a mis en place une stratégie dédiée pour renforcer son soutien aux entreprises et aux citoyens en accompagnant activement le développement de la filière dans plusieurs initiatives.[7] L'enquête locale exploratoire et qualitative, réalisée par le Groupement d'Intérêt Scientifique Marsouin, pour la Région Bretagne, s'inscrit dans le cadre de ces enjeux territoriaux. Axée sur les usages défensifs et de protection, elle fait le choix empirique original non pas de quantifier un état des lieux sur la cybersécurité des entreprises

[2] CERTFR-2025-CTI-003, Panorama de la Cybermenace 2024, 11 mars 2025. https://.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/
[3] Annexe 1 : le cadre légalAnnexe 1 : le cadre légal
[4] Annexe 1 : le cadre légal
[5] Annexe 1 : le cadre légal
[6] Annexe 1 : le cadre légal
[7] La dynamique a été engagée il y a 10 ans avec la signature, par exemple, du pacte d'avenir pour la Bretagne qui a fait de la cyber une priorité stratégique et la création du Pôle d'excellence cyber pour faire converger les enjeux civils et militaires. Dans cette optique, le Pôle d'excellence cyber (association de loi 1901) est créé en 2014 sous l'égide du ministère des Armées et de la Région Bretagne. Il a pour objectif de développer l'écosystème de la cybersécurité à partir des atouts de la Région en matière de formation, de recherche et d'entreprises innovantes dans le secteur. Lancé en 2023 par la Région, Breizh Cyber est le centre de réponse aux incidents de sécurité informatique. Dédié aux entreprises, associations et collectivités locales du territoire breton, ses experts ont pour objectifs d'analyser la menace et d'apporter un premier niveau de réponse et d'orientation des victimes vers des opérateurs installés en Bretagne. Par ailleurs, depuis 2018, la Région Bretagne a mis en place le programme BreizhFab : 2,4 M Euros de financement spécifique pour soutenir les PME industrielles bretonnes et les accompagner dans leur développement à relever 600 défis pour renforcer la compétitivité des industriels bretons, accélérer les projets de transition (environnementale, organisationnelle, numérique) et animer la communauté industrielle en Bretagne.

bretonnes[8], mais de cerner au plus près les significations données par les acteurs eux-mêmes de ces enjeux au travers de leurs perceptions, leurs actions et stratégies engagées ou non en la matière. Pour ce faire, des entreprises bretonnes de plus de dix salariés ont été identifiées et sélectionnées en amont par secteur et par taille. L'objectif recherché ici est de souligner des éléments saillants et significatifs de la question de la cybersécurité à partir de leur point de vue, celui-ci étant situé : il renvoie aussi à des éléments objectifs (secteur, taille, marché). Un guide d'entretien a été construit et thématisé selon cinq axes décrivant :

- La perception de la cybersécurité et la prise de conscience du risque cyber
- La prévention et les mesures de protection mises en place
- La gestion des incidents et la résilience
- Les investissements, normes et réglementations
- Les stratégies de entreprises en matière de cybersécurité, la gouvernance.

L'enquête a été réalisée entre le 12 février et le 16 avril 2025. Elle a connu des difficultés empiriques9 parmi lesquelles : un travail de réidentification d'entreprises (changements de nom, de direction, rachat), peu de répondants à la prise de contact renouvelée10, des refus clairement explicités (rejet de toute enquête ou sondage, le sujet lui-même, une perception de l'enquête comme d'aucun apport pour les entreprises). Au final, 11 entreprises ont répondu. Les personnes ont été interviewées via un outil de Visioconférence. Ces entretiens semi-directifs ont une durée allant de 50 minutes à 1h45. 7 d'entre eux sont issus d'une liste de 27 contacts établie par Bretagne Développement Innovation, 4 autres proviennent des réseaux d'interconnaissance professionnels ou personnels des chercheurs du GIS Marsouin. Les entretiens ont fait l'objet d'une double lecture analytique : la première « verticale » a consisté à dégager des thématiques et leurs significations propres à chaque entretien réalisé ; la seconde « horizontale » a consisté à travailler les thématiques croisées des entretiens. Les résultats sont anonymisés, ainsi que les verbatims qui sont mobilisés dans ce document.

Profil des répondants

Les interviewés sont Directeurs Généraux (3), Responsables Infra et SI (6), Responsable IT Architecture (1), Responsable RSSI et DPO (délégué à la Protection des Données) (1), Responsable Sécurité IT et OTI (1), Alternant en cybersécurité (1).[11] Parmi les entreprises répondantes au moins un des sièges (lorsqu'il y en a plusieurs) est localisé en Bretagne. Ces entreprises sont de création plutôt ancienne ; l'une d'entre elles a été rachetée par un groupe il y a un an. Elles ont entre 1 à +200 sites (avec un maximum pour une entreprise de 5 sites en Bretagne) ; 5 entreprises ont plusieurs sites, dont 3 d'entre elles sont aussi localisées à l'étranger (Europe, Etats-Unis). Elles sont de tailles différentes (entre 40 et + 20000 salariés)[12]. Cinq secteurs sont représentés par ces entreprises : industriel (2), transport logistique (2), services numériques (4), santé (2)[13], agriculture (1), agroalimentaire (1).

[8] Une autre enquête sur le sujet, quantitative, réalisée par un autre partenaire pour la Région Bretagne, est programmée au printemps 2025.
[9] Plusieurs hypothèses peuvent être émises quant aux difficultés de l'enquête : une sur sollicitation des entreprises sur une même période ? L'absence d'information initiale sur les différentes enquêtes de la Région menées par différents partenaires ? Un manque de lisibilité pour les entreprises ? Une perception de l'enquête comme évaluation ? L'absence de perception des enjeux du sujet ou l'absence de perception de ce que pourrait leur apporter l'enquête ?
[10] Sur une première liste de 27 entreprises établies par Bretagne Développement Innovation : 16 non réponses, 5 refus. Plus d'une trentaine d'entreprises (hors liste) ont été contactées ensuite mais aucune n'a répondu positivement à notre sollicitation (quelques refus et beaucoup de non réponse).
[11] Deux entretiens ont été menés avec deux interviewés.
[12] A l'exception d'une entreprise de service de très petite taille (moins de 10 salariés).
[13] Une entreprise est à la fois dans le secteur des services numériques et de la santé.

I. Une perception diversifiée de la cybersécurité par les enquêtés

La prise de conscience de la cybermenace est inégale et récente. Un basculement général s'est opéré au printemps 2020 ; la pandémie de Covid-19 provoquant un accroissement des salariés en télétravail, utilisant parfois leurs équipements informatiques personnels et augmentant ainsi la surface d'exposition potentielle aux cyberattaques. L'urgence était à la continuité de l'activité davantage que la sécurité numérique, comme le relève un rapport d'information du Sénat (2021).[14]

Pour quelques entreprises bretonnes enquêtées, l'incitation à la numérisation ou l'entrée dans un programme de transformation digitale, commencé il y a un peu moins d'une dizaine d'années, avait joué ce rôle dans un domaine qui a été sous-investi pendant longtemps : *« On est une société en transformation, ce qui fait qu'on fait un peu le grand écart en termes de système informatique […], avec « là, un mouvement intensif de changement de pratiques »* (Ent.8, transport et logistique). Pour d'autres, la cybersécurité « *c'est quelque chose sur lequel on travaille depuis déjà des années* » (Ent.10, logistique), avec des actions concrètes engagées. Pour certaines entreprises, il ne s'agit plus de savoir si elles seront attaquées ou pas, mais quand et combien de fois. La cybersécurité, pour ces entreprises, a été progressivement intégrée par les directions comme un risque croissant.

> « On évolue. En fait, il y a vraiment un focus qui est fait. Je pense que la direction générale, chez nous, a bien pris conscience déjà. Je pense que c'est un point hyper important pour les entreprises, que la direction soit consciente qu'un risque cyber, ça peut mettre à terre l'entreprise. Ça c'est quelque chose qui n'était pas, je pense, dans toutes les têtes. Nous on a travaillé pour essayer de leur expliquer qu'en cas d'attaque, comment ça se passait, on ne redémarrait pas en quatre heures. Ça pouvait durer des semaines. Donc ça, c'est un message qu'on a martelé et que maintenant, qui a été entendu. Donc il y a des actions qui sont menées. Il y a des budgets qui sont alloués aussi pour qu'on travaille et pour qu'on puisse se protéger. Donc ça, je pense que c'est quelque chose de hyper important. » (Ent.10, logistique).

Cette intensification de la question peut être liée, par exemple, au développement technologique de systèmes de capteurs ou encore de services numériques à destination des clients :

> « En fait on n'était pas, à un moment on n'avait vraiment aucun service exposé… sur Internet. Donc ça s'est développé avec la mise en place d'espaces personnels pour les adhérents et des services web qu'il a fallu mettre en place. Mais avant, le logiciel, il était accessible par VPN point basta, donc finalement on était très peu exposé. » (Ent.9, numérique et santé).

> « […] typiquement les systèmes, enfin tout ce qui est capteurs, on a besoin du Wi-Fi, on a besoin de les connecter au réseau, donc de plus en plus, donc on ne peut plus dire que ce sont des systèmes isolés, ils ne peuvent plus fonctionner en mode isolé. Donc il faut les connecter au réseau. » (Ent.10, logistique)

Elle peut aussi être assortie, par exemple, à l'étendue d'un groupe qui par de nouvelles acquisitions d'entreprises incorpore en même temps des *« zones de non confiance »*, comme le souligne un des enquêtés (Ent.10), qui décrit *« une vraie prise de conscience »* accompagnée d'actions pour pouvoir maîtriser, mettre en conformité, ou encore structurer l'infrastructure des systèmes existants sur plusieurs sites de l'entreprise, pour avoir *« une notion de groupe et d'être complètement transverse »* (Ent.7, industrie).

> « Mais c'est déjà de structurer, d'avoir les mêmes versions de logiciels partout, mais ça, c'était une spécificité, parce que [nom de l'entreprise] c'est une suite de rachats de croissance externe. Donc il n'y avait pas forcément les mêmes logiciels avec les mêmes versions partout. Là maintenant, le système d'information est transversal. C'est-à-dire que tout le monde a la même version. » (Ent.7, industrie).

> « Donc il y a un gros travail à ce niveau-là. Et puis il y a tout le quotidien en fait, tout ce qui se passe à l'extérieur et à l'intérieur puisque nos utilisateurs ce sont aussi, entre guillemets, « des points de vulnérabilité ». Donc c'est ça aussi qu'il faut qu'on adresse au quotidien. Donc il y a différents piliers sur lesquels on travaille pour justement essayer d'avoir le meilleur niveau de cybersécurité et de protection. » (Ent. 10, logistique).

[14] Rapport d'information n°678 (2020-2021), « La cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cybers virus ? par MM. Sébastien Meurant et Rémi Cardon, fait au nom de la délégation aux entreprises, déposé le 10 juin 2021. https://www.senat.fr/rap/r20-678/r20-678_mono.html

… Selon que l'entreprise est une « boîte tech » ou que « l'IT est rattaché aux services support »

Désormais la cybersécurité est un sujet pour les entreprises bretonnes enquêtées, à travers la protection de leur système informatique, au point de devenir « *une mentalité un peu globale* », précise un de nos interlocuteurs.

> « […] se protéger en cas de problème, s'assurer qu'effectivement, du point de vue du client, de se protéger, de s'assurer que l'hébergeur qui a ses données fasse correctement les choses » (Ent.2, numérique, solutions et hébergement)

Cependant l'enjeu reste perçu différemment selon qu'il est définit comme étant majeur, *« au cœur de leurs activités »* (Ent.2, Ent.9) pour des entreprises du secteur des services numériques notamment ou, au contraire, plutôt mineur c'est-à-dire *« tout sauf un enjeu du quotidien »* (Ent.6, santé). Entre ces deux pôles opposés de conception de la cybersécurité pour les entreprises enquêtées, on peut décrire des positions intermédiaires de la perception des risques selon deux autres éléments constitutifs, tels qu'ils ressortent des entretiens : des récits d'expériences d'attaques vécues ou de proximité ; la question des données.

Des récits d'expériences d'attaques vécues ou de proximité

Toutes les entreprises interviewées font référence à des événements de cyberattaque dans un contexte de dépendance accrue à l'informatique, particulièrement à l'Internet, et d'accroissement global des attaques informatiques.

> « On voit quand même globalement depuis quelques années qu'il y a eu des sociétés qui se sont fait attaquer et qui ont… Il y en a eu juste… Il n'y a pas longtemps, en plus, qui a mis la clé sous la porte suite à des attaques informatiques dont elle n'a pas réussi à se remettre. Il y a quand même un environnement qui est un petit peu anxiogène… par rapport au quotidien des attaques. » (Ent.8, secteur transport et logistique).

> « On est dans un monde où il y a de plus en plus d'informatique, où on automatise de plus en plus de choses. On est de plus en plus dépendant à l'outil informatique. Et, à la fois, c'est un outil que, on va dire, les opérationnels ne comprennent pas. […] encore même dans les équipes informatiques, c'est tellement un périmètre vaste que tout le monde ne comprend pas tout. Donc, c'est des périmètres qui sont durs à maîtriser, et en tout cas, certainement pas les personnels non techniques. » (Ent.8)

Plus que les événements parus dans les médias, ce sont les récits vécus ou d'expériences de cyberattaque d'autres entreprises proches géographiquement et/ou du même type ou secteur d'activités qui témoignent avec le plus d'acuité de la prise de conscience des risques, y compris pour les entreprises dont l'IT (*Information Technologies*) est un service support. Un des enquêtés décrit avoir vécu un *« électrochoc »*, lorsque la coopérative pour laquelle il travaillait en tant que responsable de l'infrastructure informatique, beaucoup plus importante en chiffres d'affaires et en nombre de salariés, que celle, voisine, dans laquelle il est aujourd'hui salarié, a subi *« une grosse attaque »* en 2021, alors qu'il lui connaissait *« de l'intérieur »*, *« un certain niveau de sécurité qu'on pensait en fait déjà optimal à l'époque »*.

> « Eux se sont fait attaquer et… ça a été dramatique pour la coopérative. Ils ont mis des mois à s'en remettre et nous, comme c'est une coopérative voisine, qui est basée à 30km d'ici, nous ça a fait un électrochoc en se disant mais mince on pensait avoir un niveau de sécurité suffisant mais en fait pas du tout… Comme les techniques des hackers évoluent en permanence, il faut absolument qu'on investisse et qu'on élève notre niveau de sécurité. Donc élever le niveau de sécurité et puis, surtout savoir qu'un jour on serait attaqué et donc c'est savoir comment on réagit aussi du coup, comment on redémarre, comment on surveille, comment on est prévenu de toute attaque. » (Ent.3, agriculture)

La proximité est un des facteurs de prise de conscience d'un phénomène réel : *« ça arrive même au plus gros et qui sont aussi nos voisins, ça n'arrive pas qu'aux autres et à des distances lointaines »* (Ent.3). Auquel s'ajoute une proximité pas seulement locale mais de type d'entreprise : *« une coopérative, mais voilà, à l'échelle dix fois plus grosse… et avec plus de moyens »* (Ent. 3), appartenant au même secteur d'activité. Ces récits d'expériences d'attaques rapportent ensuite les conséquences *« pas neutres »* auxquelles ont dû faire face ces entreprises, comme par exemple un licenciement de direction d'une entreprise appartenant à un groupe. Certaines parviennent à surmonter les répercussions de la cyberattaque d'envergure après des mois d'arrêt ou de ralentissement énorme de leur activité, d'autres non, comme le rapporte cet interlocuteur d'une entreprise du secteur industriel :

> « La boîte dont je parlais qui s'est arrêtée 3-4 mois c'est parce qu'elle avait des fonds d'investissements quand même assez costauds qu'elle a tenu. Nous, aujourd'hui si on s'arrête quatre mois, je ne donne pas cher de notre peau ». (Ent.5, industrie)

Ces récits remplissent la double fonction de faire prendre conscience d'une menace réelle et de jauger la capacité de sa propre entreprise à tenir dans un tel contexte, une estimation de sa propre situation en regard d'une entreprise comparable.

> « Je sais qu'il y a eu pas mal d'attaques l'été dernier, où il y a … c'était l'été dernier, je crois, notamment sur les acteurs du monde du ferry. […]. Il y a eu au moins deux sociétés, pas françaises, étrangères, mais qui ont eu des impacts opérationnels, où nous, l'infra, elle a… elle a tout absorbé, il n'y a pas eu de… Il n'y a eu aucun souci. […] on sait qu'on a été attaqués. Ça n'a pas été très violent non plus. Mais ça a été complètement absorbé par l'infrastructure sans aucun impact opérationnel. Donc, et ça, comme ça a été relayé dans les médias qu'il y avait eu des attaques pendant une semaine sur les acteurs du monde du ferry, […] qui avaient été obligés d'arrêter pendant un jour ou deux leurs opérations, nous, ça notre direction, elle a dit ah, en fait, quand même, on n'est pas si mauvais que ça et les dépenses qu'on fait pour la sécurité, finalement, c'est bien aussi. » (Ent.8, transport et logistique).

Des menaces identifiées et des risques perçus selon l'activité de l'entreprise

Les entreprises enquêtées distinguent très nettement les différentes menaces qui pèsent sur leur sécurité numérique. Parmi les principales menaces identifiées, on retrouve dans les entretiens celles liées à la cybercriminalité à travers les attaques par ransomware, l'hameçonnage ou phishing, les cryptos *(« se faire crypter les données »*, *« la prise de contrôle du SI »*, *« les cryptos monnaies »*), les intrusions dans les systèmes d'information, des menaces virales ou *BitLocker* provoquant des coupures d'infrastructure, l'activisme militant (hacktivisme), les vulnérabilités liées aux logiciels obsolètes…

> « Ça renforce quand même, le fait que… la modernisation… Il y a … enfin il y a le côté attaque, parce qu'on sait qu'on a des vulnérabilités sur notre infrastructure. » (Ent.8, transport et logistique)

> « Il y a une autre menace que je considère mais qui pour l'instant n'est pas trop présente mais qu'on ne peut pas ignorer, c'est toute la menace liée à l'activisme. Parce qu'on est dans l'agroalimentaire, donc ça génère forcément des crispations sur certaines personnes qui ont des revendications sur le bien-être animal, sur l'agriculture biologique, etc. Et vu qu'on a forcément des fournisseurs qui ne correspondent pas toujours à ces critères, donc on a des personnes qui pourraient demain s'en prendre à nous sur ces revendications-là ». (Ent.4, agroalimentaire)

Ces menaces d'ordre technique sur l'informatique de gestion sont perçues comme étant de plus en plus fréquentes et/ou sophistiquées.

> « En termes d'hébergement, on est toujours attaqué. » (Ent.2, numérique, solutions et hébergement)

La crainte par exemple d'une intrusion, liée à du ransomware ou du DDOS, *« qui viendrait paralyser ou affecter* [les] *opérations »* et rompre la continuité de service est très prégnante dans les secteurs logistique et industriel.

> « Voilà, toute la chaîne logistique. La prise de commande, les déclarations en douane parce que si un bateau, qu'il ne fait pas toutes ses déclarations, il ne peut pas être autorisé à… On a des processus manuels qui viennent renforcer les… Remplacer les dispositifs informatiques s'il y a des soucis. Mais je pense que s'il y avait… Tout n'est pas papier malgré tout. Et voilà, un bateau qui n'est pas bien déclaré en douane au ministère de l'Intérieur, aux autorités d'import-export, il ne peut ne pas être autorisé à aborder. » (Ent.8, transport et logistique)

> « Donc nous ce qui nous fait peur entre guillemets c'est la perte de continuité de service, que ça soit lié à du ransomware ou du DDOS. C'est vraiment les choses qui nous font peur. C'est vraiment les choses sur lesquelles on, parce que globalement sans IT on n'arrive pas à faire partir les camions. Donc ça c'est un des risques, un des risques majeurs. » (Ent.10, logistique)

> « Et puis, si c'est crypto, c'est couper la chaîne d'information de l'ERP[15], plus d'ERP, plus de MES[16], plus de données en temps réel, donc 5 sites qui tombent, clairement. (…). Une coupure d'infrastructure, ça peut être effectivement assez problématique. » (Ent.7, industrie).

Ce blocage potentiel total temporaire ou partiel de l'activité est aussi rapporté par les entreprises de services numériques et d'hébergement de données qui doivent *« assurer la disponibilité et la viabilité des données »* que

[15] Un système ERP (*Enterprise Resource Planning*) est un type de logiciel que les entreprises utilisent pour gérer leurs activités quotidiennes telles que la comptabilité, les achats, la gestion de projets, la gestion des risques et la conformité, ainsi que les opérations de supply chain.
[16] Le logiciel MES (*Manufacturing Execution System*) est un logiciel de pilotage de la production. C'est un système de gestion et de suivi en cours dans l'atelier. Son rôle est de superviser machines et opérateurs en fournissant une traçabilité complète des informations de fabrication.

leur confient les clients. Ces arrêts, considérés comme majeurs ou gênants, portent atteinte à leur réputation, provoquent des pertes financières ou de compromission de données sensibles. Plusieurs entretiens décalent leur propos, non plus seulement sur l'IT, mais sur le problème de l'informatique de système industriel, qui jusque-là a pu être *« un peu laissé de côté »* et peut constituer un des éléments les plus critiques, alors que ces équipements adoptent conséquemment les technologies de l'IT. La numérisation des processus industriels accroît de fait les besoins de sécurisation :

> « Là on est très focalisé IT, mais l'OTI pour moi va devenir quelque chose, va devenir un risque. Typiquement si nous on arrive à être compromis sur des éléments d'OTI sur un site, typiquement on peut changer les températures d'un site, ce qui veut dire que nos systèmes d'alarme sont neutralisés, la température sous zéro passe au-dessus de zéro, et entre guillemets c'est toute la marchandise qui devient […] détruite, donc voilà, donc ça aussi c'est un risque. » (Ent.10, logistique)

> « Nous on a quand même des équipements industriels qui ont des systèmes industriels étrangers, hollandais, allemands, pour des chaînes de calibrage, de conditionnement… Toute une chaîne d'automatismes en fait. Et ça, effectivement c'est des choses qu'on ne manageait pas trop, qui étaient plutôt gérées par l'équipe de maintenance industrielle, sur lesquelles les prestataires peuvent se connecter pour réparer quand il y a un incident. Nous, on n'était même pas au courant. Il y a un problème dans l'usine, ils appellent directement le prestataire, il se connecte, il intervient, il répare. Même s'il utilise notre réseau. Donc ça, c'est ce qu'on est en train de sécuriser cette année. » (Ent.3, agriculture)

Avec la transition digitale des secteurs industriels, l'OT (*Operational Technology*) et OTI (internet des objets, internet industriel, interopérabilité…) et l'IT convergent de plus en plus dans leurs besoins, ce qui rend compliqué la maîtrise et complexifie considérablement le métier, puisque, comme le précise un enquêté, *« le métier de l'IT et de l'OTI-IOT, c'est vraiment différent, ce n'est pas du tout les mêmes concepts, les mêmes technos et pas non plus les mêmes modes de fonctionnement »* (Ent.10).

> « Patcher un PC tous les mois, il n'y a pas de problème, on sait faire, ou un serveur, on sait faire. Donc on ne va pas pouvoir faire ça sur un capteur de température ou un automate qui fait du filmage de palettes ou des choses comme ça. Donc c'est là aussi où il faut qu'on apprenne à naviguer et à maîtriser. » (Ent.10, logistique).

D'autres menaces à la sécurité, considérées pour certaines comme étant moins contrôlables car moins techniques, plus humaines et internes à l'entreprise, sont également signalées dans les entretiens réalisés. Ce sont par exemple celles liées aux pratiques des collaborateurs, pouvant inconsidérément compromettre la sécurité numérique de leur entreprise. L'exemple parlant du personnel navigant d'une entreprise de transport et logistique, qui, embarqué pour 7 jours à bord, 24 heures sur 24, utilise les équipements de l'entreprise pour regarder des films sur leurs clés USB personnelles, avec les risques de contamination par des vers *« pas forcément perceptibles par tout le monde »*. Mais aussi l'exemple de l'usage de plus en plus répandu d'outils de l'intelligence artificielle tels Chat GPT pour accomplir un travail avec les risques de divulgation *« hors scope »* de données.

> « Des collaborateurs en général. Que ce soit sur les sites, typiquement il y a des pratiques historiques, les mots de passe qui sont partagés entre collaborateurs, on se passe les badges, enfin, voilà. Tout ça c'est des pratiques qui entre guillemets sont pour nous « à risque », l'usage privé pro, pro privé donc, tout ça pour nous ce sont également des risques et quelque chose qui de plus en plus est « à la mode » entre guillemets, c'est la protection de notre donnée, on s'aperçoit que pareil, nos utilisateurs ont des usages typiquement, c'est de dire on va peut-être parler de l'IA plus tard mais on va utiliser Chat GPT, on va utiliser des plateformes de services typiquement type Monday pour essayer de faire du travail collaboratif qui sont totalement hors scope, puisque entre guillemets moi je considère ça comme du « Shadow SaaS ». Et donc en fait on va… On va pousser de la donnée, les utilisateurs vont se créer des comptes ou s'acheter des licences et en fait ils vont commencer à divulguer de la donnée sur internet. » (Ent.10, logistique).

A l'inverse des pratiques des collaborateurs involontairement mais mécaniquement à risque, d'autres menaces internes sont, quant à elles, clairement pointées comme nuisibles à dessein, comme le vol d'informations ou de données par un employé, par exemple *« mécontent ou vengeur »* (Ent.4, agroalimentaire) qui pourrait sciemment provoquer des dommages suite à un mauvais rapport avec son employeur.

> *« Or, en interne par contre, ce n'est pas la sécu Thalès… on ne développe pas dans une cage de Faraday. Donc… et sur mon poste, c'est Internet. […] Donc, tout le monde a un téléphone portable… ça les pratiques, elles ont tellement changé. […] ça reste la personne, ça reste les personnes en interne. […]. Si j'ai envie de prendre mon téléphone portable et d'enregistrer des données que je vois sur mon écran, je peux le faire. Et il n'y a personne qui va m'en empêcher. Donc il n'y a pas de contrôle possible… »* (Ent.9, numérique et santé).

La question des données

La perception des risques est aussi directement agrégée aux *« enjeux liés à des choses qu'on nous demande de faire »* (Ent.8, transport et logistique) en lien avec les données détenues par l'entreprise, par exemple pour une entreprise reconnue OSE (Opérateur de Service Essentiel)[17]à ce jour[18], ce qui implique d'être régulièrement audité par l'ANSSI, ou, autre exemple, pour une entreprise qui mutualise le développement et l'hébergement de ressources informatiques dans le domaine de la santé (Ent.9), pour qui le règlement qui s'applique est, en plus de celui appliqué au secteur du numérique, celui relatif aux données de santé, avec les exigences juridiques et légales associées et les contrôles annuels des commissaires aux comptes de leurs clients. Les réglementations contribuent à la perception des risques en matière de cybersécurité.

> « Il y a aussi tout ce qui est un gros enjeu sur la sécurité de nos données. Et notamment, on a quand même des données qui sont assez sensibles sur nos clients. On ne les stocke pas mais elles transitent par nos systèmes. […]. Et voilà, toute cette base de données clients, voilà c'est aussi quelque chose sur lesquelles… On sécurise parce qu'on n'a pas envie que ça sorte à droite à gauche et d'avoir… Alors il y a effectivement tout ce qui est crainte d'amende liée à la non-sécurisation, à nos pratiques et à ce qui nous tombe dessus. Mais en termes d'image, ça serait aussi très dommageable à l'entreprise. Donc là, il y a quand même une forte conscience de la sécurisation. Alors, je veux dire de notre réseau, de notre patrimoine IT d'une manière générale » (Ent.8, transport et logistique)

Au-delà des menaces techniques, ce sont donc également les données que les entreprises doivent gérer qui peuvent accentuer ou non leur perception du risque.

> « Qu'est-ce qu'on a comme données ? Est-ce que c'est des données confidentielles ? » (Ent.7, industriel)

Qu'il s'agisse d'informations sur leurs clients, de secrets industriels ou de données personnelles, leur vol ou leur perte peut entraîner des conséquences tant sur le plan financier que sur la confiance des clients. La valorisation des données renforce leur importance, et par conséquent, la vigilance des entreprises face aux risques de cybersécurité. La protection de ces données devient, dès lors qu'elles sont valorisées, une priorité essentielle, car leur divulgation pourrait non seulement entraîner des sanctions légales par exemple *« liées à la non-sécurisation »* (Ent.8), mais aussi nuire durablement à l'image de l'entreprise (Ent.8). Le poids et la définition des données par les enquêtés jouent donc considérablement dans l'appréhension de la protection des systèmes informatiques, selon la centralité des données au cœur de l'activité de l'entreprise par exemple pour des entreprises d'hébergement ou de développement d'applicatifs (Ent.2, Ent.9), selon l'appartenance à la *supply chain* industrielle d'un secteur critique (par ex. défense, aérospatial, énergie) (Ent. 5, Ent.7), ou encore selon la valeur (ou la non-valeur) perçue des données en fonction de leur quantité, ou le secteur d'activité.

> « Les risques pour nous, ça peut être une perte de nos données. Donc, ça, ça aurait un impact sur l'outil de production forcément, le temps de remettre les choses en route. Voilà le principal risque pour nous, on va dire le principal risque direct. Mais il n'y a aucune… On aurait juste un délai, le temps de remettre le système, de recharger le système, si vraiment on avait une perte de ce qu'on a. Après la valeur de nos données, nous, il n'y en a pas en fait. […] . Je peux donner tout ce qu'on possède à quelqu'un, je ne sais pas ce qu'il en ferait, mais ça n'aurait aucun impact pour nous. […]. Il n'y a pas de secret industriel qui serait dévoilé ou quoi que ce soit. […]. Après on héberge forcément des données de santé sur nos patients donc ça a un impact pour nos patients si ces données étaient volées ou si elles étaient utilisées par quelqu'un pour quoi que ce soit. » (Ent.6, santé)

Les enquêtés procèdent à une forme d'évaluation de la probabilité du risque, comme le montre ce témoignage estimant que *« les chances que ça arrive sont extrêmement faibles »*, d'autant plus que *« les données récupérées ont un intérêt extrêmement limité »* (Ent.6), qu'elles sont peu nombreuses :

> « Bon ! ça ne représente pas non plus grand-chose. Ce n'est pas des quelques milliers de patients qu'on a sur toutes ces années et des données qui ne sont pas forcément très sensibles non plus. Par exemple, il y avait une société d'assurances qui a été piratée l'année dernière, voilà on parle de millions de personnes concernées, on n'est pas à la même échelle. » (Ent.6, santé).

[17] L'opérateur de services essentiels élabore, tient à jour et met en œuvre une politique de sécurité des réseaux et systèmes d'information (PSSI). Cf. Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique. NOR : PRMD1824939A. JORF n°0225 du 29 septembre 2018.

[18] Cette terminologie (OSE) évolue avec la directive NIS 2 : entités essentielles et importantes.

La mesure de l'impact et de la probabilité se rapproche de la logique d'une analyse de risques. Mais la question des données peut aussi être bien plus complexe qu'elle n'y paraît, particulièrement lorsqu'elle renvoie à la circonscription des données d'entreprise, comme l'interroge particulièrement cet enquêté :

> « Et bien justement, moi je n'arrive pas à maîtriser quel type de données, potentiellement il peut y avoir de la donnée client, typiquement il peut y avoir, je ne sais pas moi, des contrats clients, on va envoyer un contrat client dans Chat GPT parce qu'on veut une synthèse de ce que le client va demander en fait, quels sont les points pertinents de l'appel d'offres par exemple. Donc là, il y a tout un tas d'informations, ça peut être aussi des comptes rendus de réunion, enfin je ne sais pas, donc en fait il y a tout un tas de données, ça peut être de la donnée client, de la donnée interne et en fait c'est le fait de ne pas savoir, pour moi c'est ça aussi le risque, c'est qu'on sait qu'il y a des choses qui sortent et en fait ça peut-être de la donnée pour moi sensible. » (Ent.10, logistique).

La donnée peut donc avoir une définition extensible, plus ou moins indéfinie : *« notre donnée, on sait que c'est quelque chose qui appartient à l'entreprise et le fait de la diffuser on ne sait où, sur des plateformes et bien derrière on perd la main dessus »* (Ent.10). Ce risque est également identifié par un autre interlocuteur à propos des fuites possibles de données dès lors que certains logiciels utilisés ne sont plus localisés « en interne », mais « sur le web », des plateformes qu' « *on ne maîtrise pas* ».

> « Donc, en fait les données elles ne sont plus sur le SI interne, elles sont, donc je ne sais pas trop où, voilà, donc en gros là, pareil il faut bien lire les contrats pour savoir où sont les données en espérant que ce qui est marqué est vrai. […]. On est obligé de rester en Europe. On est obligé et moi, je n'aime pas les données, nos données elles ne sortent pas, mais il y a toujours des fuites possibles puisque les logiciels pour faire de la conception ou des diagrammes ou je ne sais pas trop quoi, maintenant, potentiellement, ce n'est plus en interne, c'est sur le web » […], « on a vite fait de mettre des données personnelles sur ce type de logiciel. On ne sait pas trop, même sans le vouloir, on ne s'en rend pas trop compte, il y a des données qui fuitent, c'est un peu moyen, et en plus ne serait-ce que la gestion des comptes lors des départs, c'est tout un problème parce qu'en gros, il n'y a pas une gestion centralisée des accès, et savoir qui avait accès à quoi, ce n'est pas si simple que ça. C'est des choses qui paraissent ultra simples, quand on commence à avoir 20-25 logiciels SaaS qu'on ne sait pas qui a accès à quoi, il faut faire des revues de ces trucs, ça prend un temps fou, et c'est accessible pour le coup-là, il faut clôturer les accès assez rapidement, puis c'est accessible partout, donc hors interne, c'est vraiment ça fait partie des choses qui sont compliquées à gérer, typiquement. Il y a très peu de logiciels d'éditeur SaaS qui donnent des comptes, des accès qui sont à l'IPEC ou qui sont reliés à des ID externes, c'est souvent des comptes internes, accessibles partout dans le monde, c'est compliqué. C'est un truc qui paraît simple, ça depuis deux ans ça devient problématique ». (Ent.9, numérique et santé)

> « Après il y a la problématique IA, on ne peut pas, c'est un peu dans la même lignée, un peu des logiciels SaaS, au pire potentiellement, parce que le logiciel SaaS il était un peu borné au niveau de l'utilité du logiciel. Le Chat GPT et le Mistral AI on peut lui poser tout et n'importe quoi de nos questions, et là, il va mettre tous les documents de la terre et du SI en entrée, il sera très content, et savoir qu'est-ce qu'ils font derrière, c'est compliqué. » (Ent.9, numérique et santé).

L'IA apparaît de surcroît dans les discours comme une problématique émergente et qui questionne beaucoup la maîtrise, (c'est-à-dire la perte de la main mise et sonde indirectement une part de leurs compétences professionnelles), le périmètre de sécurisation de leurs données. Ce questionnement du fait des usages de plateformes ou d'outils de l'IA, interroge le périmètre de l'entreprise *par ses données.* Elle élargit tout en rejoignant, en ce sens, des problématiques, déjà existantes, sur la question des frontières de l'entreprise et leurs transformations comme organisation (numérique) du travail. Ce à quoi les entreprises constituées de plusieurs sites, situés dans plusieurs pays, avec différents métiers et un fonctionnement en silos assez fort, sont d'autant plus soumises pour protéger les systèmes et essayer de formaliser la sécurité.

> « Après l'évolution, elle n'est pas liée seulement à la menace, elle est liée aussi à l'écosystème informatique. Avant, vous aviez le réseau de l'entreprise qui était sanctuarisé, protégé au niveau périmétrique, des utilisateurs qui étaient dans le réseau de l'entreprise, et les serveurs et les ressources qui étaient dans le réseau. Maintenant, on a le télétravail, on a des gens en nomadisme, on a également des ressources qui sont en SaaS sur internet, et tout ça apporte un vrai flou sur le périmètre de l'entreprise. » (Ent. 4, agroalimentaire).

En résumé : la prise de conscience des entreprises face au risque cyber est inégale et relativement récente. Elle est liée au développement technologique (l'informatique des systèmes industriels ou des services aux clients, par exemple) ou à l'augmentation de la surface numérique sensible (la croissance d'un groupe, le développement du télétravail ou l'utilisation des logiciels SAAS, par exemple). Les récits d'attaques vécues par d'autres entreprises du même secteur d'activité ou géographique accélèrent cette prise de conscience. De même, la valorisation des données renforce la vigilance des entreprises face aux menaces cyber, *a fortiori* dans un contexte de nouveaux usages liés à l'IA.

II. Des mesures de prévention et méthodes de protection mises en place par les entreprises

Qu'elle soit progressive et propre à l'entreprise, qu'elle s'impose par les réglementations, ou encore, qu'elle soit orientée sous forme de consignes par le secteur d'activités dans le cadre d'un programme industriel par exemple, la prise de conscience des risques conduit les entreprises enquêtées à mettre en place des mesures de prévention et des méthodes de protection pour faire face au risque cyber.

> *« On a un gros volet sur le 4.0 avec le programme industrie du futur du GIFAS. Donc le GIFAS, c'est le Groupement des Industriels Français de l'Aéronautique et du Spatial. Et dans ce cadre-là, on est challengé sur un programme qui s'appelle Boost Aerospace, qui est donc Airbus, Safran, Thalès et Dassault, qui nous challenge sur la partie cybersécurité. (…]. Et donc de ce fait, on est challengé, on est audité, on est accompagné sur ce programme, avec trois niveaux Bronze, Argent et Or, avec des paliers avec des critères à respecter pour être dans l'un et des critères un peu plus restrictifs pour le niveau supérieur et encore plus restrictif pour le dernier, pour l'Or. […]. Là désormais, depuis Octobre 2023, on est bronze. Et là, l'objectif que m'a donné la direction, c'est d'atteindre le niveau argent pour la fin de l'année. »* (Ent.7, industrie).

Il s'agit d'une démarche graduelle, à partir de l'existant, qui peut procéder d'abord par une autoévaluation sous forme de questionnaire : *« les règles d'hygiène et de sécurité de base de l'ANSSI que toute entreprise devrait avoir »* (Ent.5, industrie), tels qu'en rendent compte les guides essentiels et les bonnes pratiques édités par l'Agence Nationale de la Sécurité des Systèmes d'Information par exemple[19]. Cette première autoévaluation peut donner lieu notamment à une validation de *Maturity Assessment* de la part de donneurs d'ordre qui établit à quel niveau se situe l'entreprise *« en début de course »* (Ent.5, industrie). Pour construire ensuite sur plusieurs années, étape par étape, selon des exigences propres par exemple aux différents secteurs d'activité, une politique de gestion du risque numérique au sein de son entreprise.

> « C'est un groupe de travail, puisqu'on a des échanges tous les mois avec eux, où on fait le point, […]. A côté de ça, on a un catalogue, […], toutes les applications et technologies et éditeurs au sein de ça, qui s'appelle le cyber catalogue. » (Ent. 7, industrie).
>
> « On répond avec des outils qu'on installe » (Ent.7).
>
> « On a aussi des *extend*, des extensions à ce questionnaire pour des clients spécifiques, qui demandent plus de sécurité encore dans ce domaine précis. » (Ent.5, industrie)

Plusieurs entreprises enquêtées, particulièrement du secteur du numérique, sont dans une démarche de certification ISO 27001[20] en cours (Ent.2), ou l'ont déjà obtenue et l'ont renouvelée depuis (Ent.9). La certification initiale recouvre un cycle de trois années, avec le déroulement d'un audit qui a lieu tous les ans où *« on prouve tout notre périmètre d'activité ».*

> « Ça sert énormément, ça sert énormément. Puisqu'on va dire, il y a un cycle d'amélioration continu qui, quand on me l'a présenté me faisait doucement rigoler, on est obligé de le faire. Puisque les auditeurs, ils vont trouver qu'il y a des non-conformités majeures, c'est bloquant, mais il y a des mineures, des points sensibles. Les points sensibles, si on ne les traite pas, ils deviennent des mineurs. Et les mineurs, si on ne les traite pas, ils deviennent des problèmes majeurs qui te bloquent. […]. Donc tu es obligé de t'améliorer. Et ce n'est pas un ou deux points sensibles qu'on se prend chaque année, c'est une pelle. Donc une pelle de points sensibles. En plus on est obligé de faire un audit interne équivalent à l'audit de 27001, mais par un autre auditeur, mais qui n'est pas de l'organisme de certification. » (Ent.9, numérique et santé).

Ce *« processus continuel »*, *« en train de se faire »*, d'une évolution permanente dans le temps *(« on progresse »*, *« on évolue »*) des technologies et d'amélioration des niveaux de sécurisation, se traduit pour les entreprises enquêtées par la mise en place de différentes actions de protection cyber suivant trois orientations :

---

[19] https://cyber.gouv.fr/guides-essentiels-et-bonnes-pratiques-de-cybersécurité-par-ou-commencer ; https://cyber.gouv.fr/les-essentiels-de-lanssi

[20] ISO/IEC 27001 est la norme la plus connue au monde en matière de systèmes de management de la sécurité de l'information (SMSI). Elle définit les exigences auxquelles un SMSI doit répondre. La norme ISO/IEC 27001 fournit aux entreprises de toutes tailles, quel que soit leur secteur d'activité, des lignes directrices pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de management de la sécurité de l'information. La conformité à ISO/IEC 27001 signifie qu'une organisation ou une entreprise a mis en place un système pour gérer les risques liés à la sécurité de ses données ou des données qu'elle est amenée à traiter, et que ce système est conforme aux bonnes pratiques et principes énoncés dans cette Norme internationale.

technologique et technique (axées sur les outils), organisationnelle (axée sur les méthodes de gestion du travail et de la sécurisation) ; et informationnelle (le suivi et la veille professionnelle, la sensibilisation).

Des technologies et techniques de protection des systèmes

Les entreprises enquêtées inventorient d'abord les outils technologiques et techniques installés afin d'évaluer les risques, puis en implantent d'autres pour renforcer leur sécurité.

> « Sans rentrer dans les détails, c'est déjà d'avoir l'énumération de tous les outils. Des cascades de remise en service de chaque outil, parce qu'il y a des outils, il faut les mettre dans un certain ordre parce que ça s'implique dans un certain ordre, il y a des criticités en fait, vous partez d'une matrice de risques, vous faites votre catalogue La redoute de tous les logiciels que vous avez dans la boutique et après de se dire si cette couche-là je ne l'ai pas ça impacte qui ? Quel est le délai dans lequel il faut remonter, et ainsi de suite. Donc c'est surtout, c'est une matrice d'évaluation des risques. Il faut se baser là-dessus. Et toute la sécurité cyber, c'est une matrice d'évaluation des risques. » (Ent.7, industrie).

Toutes les entreprises enquêtées ont mis en place *« différentes couches »* externe et interne (Ent.9, numérique et santé) d'outils de sécurité de leur système informatique de gestion, allant des plus *« évidents »* ou *« classiques »* tels les pares-feux (*firewall*), les antivirus, les antispam, les mails box, *« des proxys, des reverse proxys »,* la sécurisation des sauvegardes sur différents supports informatiques (serveurs physiques et sauvegardes en ligne, sauvegarde immuable), l'accès au réseau et aux données (nécessité d'être soit sur le réseau physique ou sur le VPN ; l'utilisation de solutions d'authentification forte ou double authentification ; bastion), etc., aux systèmes plus spécifiques de détection et de réponse (EDR , XDR, SOC, SIEM), des systèmes de gestion des informations et des événements de sécurité, tels le SIEM (*Security Information and Event Management*), une solution de sécurité qui permet aux organisations de détecter les menaces avant qu'elles ne perturbent leurs activités.

> « Alors nous, en fait, on a la chance d'avoir mis en place un SOC. Nous, on repose sur un SOC pour justement avoir cette détection… Donc on a mis en place aussi des systèmes sur tout un système d'EDR. On collecte un certain nombre de sources pour justement fournir beaucoup de data au SOC pour qu'il puisse corréler et pouvoir détecter les signes faibles et nous alerter en cas d'événement suspect. Donc ça, c'est notre brique de base. » (Ent.10, logistique).

> « Le SIEM, c'est vraiment pour moi, voilà, après… après on peut tout maîtriser, voir, pour faire les actions parce qu'on peut tout maîtriser quand on est plus mature […]. » (Ent.9, numérique et santé)

Certains outils technologiques en place peuvent être anciens et côtoyer, au sein d'une même entreprise, d'autres outils qui sont, au contraire, en pointe. Les EDR et XDR sont, par exemple, des solutions de cybersécurité basées sur l'*IA* et l'automatisation. Ces nouvelles technologies d'IA intégrées dans les mécanismes logiciels sont décrites comme *« des outils de plus en plus puissants, de plus en plus complexes, mais qui demandent une vraie expertise dans leur gestion »* (Ent.4, agroalimentaire), pas toujours présente au sein de l'entreprise, ces outils requièrent alors le recours à des prestataires externes. Ils peuvent également faire l'objet de critiques de la part d'enquêtés, pourtant professionnels du domaine de la sécurité informatique et de la protection des données, dès lors, souligne l'un d'eux qu'« *on ne comprend plus ce que ça fait, soyons clairs* ».

> « On ne comprend absolument pas ce que le logiciel fait puisque, je prends un cas simple, le bannissement de l'IP, en gros, c'est le logiciel qui va décider que l'IP a fait des requêtes excessives. Mais il n'y a pas un seuil. […] Et comment il trouve ? On ne peut pas dire. Si je demande au constructeur de l'IA. Ah non, c'est l'IA. L'IA, elle fait quoi ? En fait, il n'y a pas un seuil, donc en fait on a du mal à savoir exactement ce qu'ils font. Alors ça doit marcher. On va supposer que la boîte de logiciels ils savent ce qu'ils font. Mais il y a ce côté un petit peu frustrant où des fois on ne comprend pas ce que ça fait » (Ent.9, numérique et santé).

Un des enquêtés évoque ce *« grand écart en termes de système d'information »* au sein de son entreprise avec le centre de leur activité qui est piloté par deux ERP de plus trente ans d'ancienneté et un tiers de l'infrastructure *« cloud native »*, qu'ils sont *« en train de migrer dans des environnements cloud publics, avec des technos modernes, du Kubernete, des choses qui sont de l'infrastructure AS-Codes »*, renvoyant à des pratiques actuelles : *« un Kubernete complètement automatisé, scalable, bien protégé »*, *« des choses qui sont plutôt de l'état de l'art des pratiques de ce qui se fait maintenant »* (Ent.8, transport et logistique).

> « […] dans ces vieux systèmes, tout n'est pas forcément aux normes. Et quand c'est des systèmes qui sont très connectés à d'autres choses, des fois c'est… C'est compliqué. Mais on fait évoluer au fur et à mesure des découvertes. Parce qu'on découvre un petit peu de tout, tous les jours des nouvelles choses aussi sur des trucs internes. On progresse. » (Ent.8, transport et logistique).

Hériter d'un patrimoine technologique ancien peut rendre plus difficile la sécurisation des systèmes, comme le souligne cet enquêté : *« c'est plus facile de construire de zéro, effectivement, que d'hériter d'un patrimoine »* (Ent.8). A ce problème d'ancienneté de certains systèmes s'ajoute celui du déploiement d'une technologie homogène pour une sécurité uniforme pour l'ensemble des utilisateurs d'un groupe, comme par exemple des projets en cours de protection des terminaux mobiles, ou d'accès au système d'information pour les fournisseurs avec la mise en place de solution de type bastion, ou encore des solutions de sécurité dans des services Saas, Cloud. Ces choix sont souvent justifiés par les enquêtés par *« la maîtrise »* et la possibilité d'« *avoir un niveau de contrôle »* (Ent.10).

> « Moi, ma problématique c'est, j'avais une bonne vision de ce qui se passait en France puisque les équipes elles sont dans le même bâtiment que moi, j'ai la problématique de voir ce qui se passe en Espagne, en Italie. Je ne sais pas ce qui se passe sur les sociétés nouvellement acquises, comment ils sont interconnectés. Et moi, ça, c'est une problématique, parce que je ne peux pas sécuriser quelque chose que je ne connais pas. […]. L'idée c'est d'homogénéiser et d'avoir quelque chose de centralisé. » (Ent.10, logistique)

Le fait d'avoir des outils unifiés, permet donc d'avoir un meilleur contrôle, qui ne repose pas uniquement sur la déclaration du suivi des préconisations. On retrouve cette difficulté dans des entreprises de secteurs différents, notamment ceux de l'industrie, la logistique ou l'agroalimentaire, qui toutes ont en commun d'avoir plusieurs sites. Cette notion de contrôle est aussi présente dans le choix des outils de gestion de la sécurité. En effet, le choix des logiciels en cybersécurité semble se porter plutôt sur des produits d'éditeurs *« souvent un leader du marché »*, dont la notoriété est reconnue parce-qu'« *avec les normes qu'on a, moi les petits fournisseurs ça ne m'intéresse plus »* précise un enquêté (Ent.9, numérique et santé) :

> « C'est-à-dire qu'on nous demande d'être certifiés, on est audité, on nous demande des certifications et de prouver qu'on fait bien les choses. C'est aussi de demander à nos sous-traitants de faire ricocher. Et donc en fait moi, en gros, les sous-traitants qui ne sont pas certifiés, ils m'embêtent aussi puisque j'ai pas envie de passer trois jours à les auditer. Donc, en fait, finalement, la seule solution qui est entre guillemets « acceptable » pour tout le monde, c'est la certification. Le mec, il a été certifié par un auditeur indépendant. Bon, c'est bon, j'ai confiance en mon auditeur et je vois ce que ça donne chez moi. Donc je sais qu'il fait bien son job. Donc il n'y a pas de souci. » (Ent.9, numérique et santé).

Un outil *« qui est simple à manager pour ne pas être obligé d'avoir une équipe derrière de spécialistes »*, tout en conservant *« notre autonomie sur notre système d'information »*, *« on veut garder la main aussi sur la solution utilisée »* (Ent.7 ; Ent.9). Parmi les entreprises enquêtées, particulièrement des industries appartenant à la *supply chain* de secteurs de données critiques, des entreprises du numérique ou du secteur de la logistique, il s'agit souvent d'avoir un soutien, mais sans perdre le contrôle : *« c'est-à-dire qu'aucune des fonctions de sécurité ne sera intégralement sous-traitée »* (Ent.7). Ceci implique la structuration au sein des entreprises d'un service informatique avec au moins un poste, voire une équipe dédiée, tout en recourant à des prestataires.

> « Moi je veux pouvoir ajouter, supprimer des utilisateurs sans être obligé d'ouvrir un ticket, où on paye au ticket, où on a quatre heures de résolution de ticket. Je me connecte sur le système, j'ajoute mon utilisateur et je suis autonome. […]. Donc c'est des outils tout simples, mais il faut le poser dans le cahier des charges quand vous choisissez une solution » (Ent.7, industrie).

> [À propos du suivi du SIEM qui se fait « en interne »] « Le fait de l'avoir en interne au moins on sait ce qu'on fait et ce qu'on ne fait pas » (Ent.9, numérique et santé)

Y compris, par exemple, comme le précise un enquêté, sur des technologies d'infrastructure Cloud centralisées (ex. Google Cloud) *« pour rationaliser les pratiques »*, mais où la compétence reste internalisée :

> « Parce que c'est quand même le cœur de notre activité. Donc aujourd'hui on est sur cet aspect-là autonome. Mais c'est un peu… Je ne vais pas dire que c'est une exception. Mais généralement, on essaye d'avoir au moins une personne interne sur un sujet sachante. Et puis, par contre, le travail est souvent externalisé avec des… Voilà un partenaire, enfin un ensemble de partenaires spécialisés dans ces différents sujets. » (Ent.8, transport et logistique)
> « Ce n'est pas Open bar quand on est dans notre réseau, au moins dans notre cloud. Pareil sur le réseau interne, je pense qu'il y a des isolations aussi, mais elles sont moins fortes que ce que nous on a mis en place dans la partie cloud. L'infra elle est résiliente par design, elle est encode. Je ne vais pas dire qu'en deux clics on peut remonter l'infrastructure à côté s'il y avait un gros souci, mais normalement… Il y a des petits points réseau qui ne sont pas encore complètement automatisés, mais on va dire que 99% de l'infrastructure, enfin l'infrastructure cloud, on sait la redéployer de manière identique et totalement automatisée. » (Ent.8).

Pour *« savoir ce qui se passe »*, *« ne pas être complètement les mains liées au partenaire »,* ne serait-ce que pour conserver ses données, particulièrement si elles émanent d'infrastructures critiques, pour lesquelles, *« les mettre dans le Cloud »*, ne garantit pas l'hébergement en Europe et réclame davantage de preuves (Ent.7, industrie) :

> *« Il faut en avoir la garantie, il faut vérifier. Parce que les données, les données vous pouvez les passer… les gens qui sont en full SaaS, les données maintenant avec les données maintenant avec les équipements actuels, un système d'information peut les faire tourner et les faire passer d'un Data center à un autre sans que l'utilisateur, à l'autre bout, s'en aperçoive. C'est du temps réel. On est capable, à chaud, de faire travailler une équipe sur un équipement qui est mouvant, parce qu'il passe d'un Data center à un autre. Là, comment vous pouvez justifier ? » (Ent.7, industrie).*

Et des méthodes d'évaluation de ces outils

L'implantation et l'utilisation d'outils technologiques et techniques pour assurer la cybersécurité implique ensuite le développement de méthodes d'évaluation des systèmes déployés.

> « Donc il va falloir qu'on mette un plan de bataille là-dessus. Mais j'ai des outils, il y a déjà des outils pour se blinder. […] En fait, c'est ça, la première étape c'est de se blinder. Et puis après on teste le blindage voilà. » (Ent.7, industrie)

Parmi ces méthodes, des audits de sécurité internes peuvent consister *« à casser l'applicatif en cours de développement par des tests d'intrusion »*, *« par des méthodes de sécurité un peu habituelles de hack »*, *« en boîte blanche »* pour faire davantage d'audit de code, pour ensuite *« améliorer les techniques de développement aussi derrière »*, comme le souligne un des interlocuteurs d'une entreprise du numérique et d'hébergement de données (Ent.2). Les équipements installés, de type SOC ou SIEM, constituent des *« outils d'audit »* internes, en remontant les informations, ils permettent d'obtenir une traçabilité des événements qui se sont produits. Des évaluations internes et des audits externes scannent la vulnérabilité.

> « Donc, ça, c'est un autre principe. C'est on va dire, la partie audit et vulnérabilité. Donc en fait, on a des scanners de vulnérabilité qui soient internes ou externes. Donc externes pour évaluer notre niveau de maturité vu d'Internet. Parce qu'en fait, ça aussi, c'est une pratique qui est arrivée. C'est que ce type de scanner, en fait, est utilisé par les cyberassureurs, pas uniquement par les attaquants, mais aussi par les contrôles de gestion et les cyber assureurs. […] Donc c'est pour ça que c'est quelque chose aussi de visuel et c'est pour ça aussi que ça attire l'attention de la direction. Et donc, on est aussi vigilant à voir quelles images on montre à l'extérieur. »

> « Donc ça c'est la partie externe et on a tout un tas de scans, internes, pour évaluer, détecter les vulnérabilités et tenter la remédiation le plus rapidement possible. Et il y a aussi toutes les prestations, on va dire, d'audit externe. Typiquement nous, on n'a pas, au niveau de la SSI, on n'a pas un rôle, on va dire d'attaque. On est plus en mode protection, gouvernance. Et donc, on fait appel à des sociétés externes pour faire du Pen test et de l'audit sur différents périmètres applicatifs ou autres. » (Ent.10).

Des experts interviennent pour réaliser des tests de vulnérabilités, des audits de configuration ou des tests d'intrusion (*Penetration Tests*) notamment, permettant d'identifier et de corriger rapidement les failles potentielles. Des campagnes régulières de « *bug bounty »* peuvent être orchestrées avec des sociétés extérieures spécialisées dans ces tests, *« sur un périmètre qu'on définit, on leur dit, allez-y, attaquez-nous, essayez de chercher des failles »*, comme le précise un enquêté (Ent.8, transport et logistique).[21]

> « En X heures ou X jours, il a réussi à se connecter à tel environnement. Derrière il a rebondi. Et en fait, il a réussi à faire différents chemins d'attaque. Donc derrière, il y a un plan de remédiation bien sûr. Mais ça, c'est hyper visuel et c'est hyper intéressant. Donc ça, on va le refaire d'ici quelques temps ». (Ent.10, logistique)

Ces tests d'intrusion servent de preuves de la vulnérabilité ou pas. Ils permettent de déceler des chemins qui n'avaient pas été identifiés et de *« vérifier la chaîne de supervision »* (Ent.10). Ils débouchent sur un plan de remédiation qui peut consister à monter des projets de déploiement de nouveaux outils… La démarche d'audits externes ne se limite pas à la vérification documentaire. En simulant des attaques pour tester la résilience des systèmes, elle est utilisée pour évaluer la maturité de la sécurité, à distance, en réponse aux exigences des contrôles réglementaires ou de normes (ex. ISO 27001), ou des cyberassureurs. Elle implique donc des tests opérationnels en situation réelle, afin d'assurer la robustesse et la réactivité des dispositifs.

> « C'est la norme qui oblige de faire un audit interne de la norme ». « Et après, ils vont demander les audits des intrusions. Et en fait, il y a énormément d'améliorations prises en compte. J'ai un fichier d'améliorations continues depuis, je ne sais pas en quatre ans, je pense que j'ai 300 ou 400 points de traité. C'est énorme, on va dire. Et je n'ai pas du tout noté au début. Donc, le nombre,

[21] https://www.numerique.gouv.fr/actualites/le-bug-bounty-un-dispositif-innovant-pour-renforcer-la-securite-des-services-numeriques/

> de points traités, c'est incroyable comment on est obligé de s'améliorer. Et fatalement, ça prend du temps. C'est sûr que ça ne va pas passer du jour au lendemain. Il faut dire, on va mettre 5 ans. […] C'est long quand on a une menace qui est urgente. C'est-à-dire qu'on n'a vraiment rien et qu'on est attaqué tous les jours. Mais au final, on a un truc qui tient à la marée. On a réellement un truc qui marche. Et entre le début de la certification et maintenant, c'est plus qu'un gap. Il y a un monde d'écart. » (Ent.9, numérique et santé).

> « C'est vraiment de l'opérationnel c'est pas une analyse de risques et des grands principes, c'est vérifier que ça marche. Donc avec des tests, en live, on intègre un flux, on met des erreurs, on voit que c'est bloqué, on fait planter un traitement, on vérifie qu'il y a une alerte, etc. C'est des cas qu'on passe avec eux et qui n'est pas du tout de la doc. Pour le coup, contrairement à 27001, ce n'est pas des analyses documentaires, c'est devant le PC à faire des tests. » (Ent.9, numérique et santé).

L'installation de systèmes de protection des systèmes d'information et des données, puis leurs évaluations récurrentes, les plans de remédiation, attestent d'un processus itératif, jamais achevé, avec des technologies en perpétuelle évolution, et des normes et certifications qui suivent ou s'adaptent à ces évolutions techniques :

> « Et il y a eu un sacré gap avec la nouvelle version de la norme [ISO 27001]. La 2022. » (Ent.9, numérique et santé).

Les méthodes de protection organisationnelles pour la gestion des incidents

L'intégration de ces exigences normatives et techniques s'appuie sur l'organisation de l'entreprise. Plus ces mesures de prévention d'ordre technologique et technique sont développées, plus elles semblent s'adosser à la production des méthodes de protection formalisées au niveau de l'organisation de l'entreprise : des plans de gestion de crise, de reprise d'activité (PRA) ou de continuité opérationnelle… vers l'élaboration progressive d'une vision stratégique ou de futures politiques de sécurité des systèmes d'information (PSSI)[22]. La mise en place d'un cadre organisationnel structuré adapté ou en cours de structuration, appuyé, pour certaines entreprises enquêtées, sur des référentiels d'exigences de sécurisation et de fiabilité du système d'information, qui peut être par exemple un programme établi par des donneurs d'ordre du secteur d'activité industriel, ou des certifications, comme la norme ISO 27001, constitue pour ces entreprises une étape fondamentale en termes d'actions, d'écriture et de mise en place de ces procédures internes.

> « Il faut mettre en place des procédures », « on est accompagné effectivement dans le cadre de nos donneurs d'ordre » (Ent.7, industrie)

> « C'est beaucoup écrire les procédures qu'on met en place […]. Et c'est décrire tout ce process… C'est un exemple de ce qui est demandé dans cette certification » (Ent.2, solutions numériques et hébergement)

Toutes les entreprises enquêtées n'ont pas conçu à ce jour de plan de gestion de crise cyber, *« pas encore »* précise un enquêté qui ajoute que c'est en prévision sur le budget 2025 (Ent.3, agriculture). L'élaboration d'un inventaire des systèmes d'information déployés au sein de l'entreprise, en relation avec les différents métiers qui les utilisent et pour quelle activité, peut amorcer l'établissement d'un plan de reprise d'activité. Ce premier élément permet d'évaluer à partir de combien de temps l'indisponibilité d'un système devient critique pour l'activité de l'entreprise, afin notamment de prioriser en cas d'un incident conséquent la remise en service des systèmes les plus importants au fonctionnement (Ent.4, agroalimentaire). Ces plans *« de secours »*, souvent élaborés avec l'aide de cabinets spécialisés, visent à garantir la capacité de l'entreprise à résister et faire face à une attaque cyber ou tout type de dommages, en décrivant les process qui permettent de remonter les systèmes en question, à partir de la documentation de ces systèmes qui doit être décrite en amont. Le but étant de produire un document lisible *« y compris en termes de gouvernance par la direction »* (Ent.7, industrie). Une partie jugée parmi les plus complexes par les enquêtés.

> « Il y a un plan de gestion… Là on a monté, sans rentrer dans les détails, un plan de reprise d'activité. Là on a été accompagné par BreizhFab, le programme BreizhFab[23] sur cette partie Cyber, par un consultant qui m'a accompagné pendant 5 jours sur 3 mois, sur monter carrément un plan de reprise d'activité, monter un PRA. Et de faire un outil où on référence tous les logiciels, toutes les applications entre eux, tous les flux d'informations. […]. Ce qu'il y a c'est que, quand on est informaticien, toutes ces choses-là, on l'a. J'allais dire c'est un défaut, c'est un défaut de la profession informatique. C'est qu'on l'a dans la tête, on sait comment ça fonctionne. Maintenant le but, c'était de faire un document lisible, y compris en termes de gouvernance par la direction.

[22] https://cyber.gouv.fr/publications/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation
[23] https://www.breizhfab.bzh/

> […].[…]. Donc c'est une approche, ça permet de structurer et d'avoir une lisibilité du système d'information autre que par les gens du Sérail. » (Ent.7, industrie).

Pour certaines entreprises enquêtées, *« sur le papier »*, *« tout le monde connaît son rôle et sait où trouver cette documentation »* (Ent.4, agroalimentaire), *« une cellule de crise est identifiée »* (Ent.8, transport et logistique), avec un *« coordinateur de crise »* (Ent.10), avec des procédures établies notamment en matière de communication et de coordination sécurisée, complètement déconnectées, pour une entreprise qui s'est construite sans IT par exemple, pour travailler la continuité de l'activité :

> « Il y a un plan de continuité d'activité, il y a un plan de gestion, il y a une cellule de crise qui est identifiée. Alors, je ne vais pas dire, on a des outils, on est en évaluation d'une suite d'outils complètement déconnectés de notre SI pour gérer de la communication du… que ce soit en visio comme on fait, du partage du fichier, du partage de mails, des to-do list, etc. qui est un système qui est limité à une trentaine de personnes, 30-50, enfin je ne sais plus le nombre exact de personnes pour justement en cas d'attaque majeure, de défaillance majeure de tous nos systèmes informatiques, d'avoir des canaux de communication, d'organisation, de coordination sécurisée et complètement déconnectés. Ce n'est même pas connecté à notre Active Directory, ce n'est pas connecté au réseau, c'est connecté à rien du tout. » (Ent.8, transport et logistique).

D'autres, plus rares, vont jusqu'à réaliser des exercices de gestion de crise pour essayer de se préparer et tester ainsi leur capacité à répondre à partir de scénarios (Ent.10, logistique).

> « On sait que ça nous arrivera […], et certainement avec une envergure beaucoup plus importante. Donc, on essaye de se préparer. On se prépare… Alors, comment dire ? On fait appel à des cabinets pour faire des exercices de gestion de crise. […]. Parce que l'entrainement c'est quelque chose d'important. On a aussi toute une mallette de gestion de crise. » (Ent.10).

Ces exercices réguliers de gestion de crise, simulant des scénarios variés, permettent de tester la capacité des équipes à réagir efficacement, en mobilisant *« une mallette d'outils »* (Ent.4, agroalimentaire) et de procédures. Ces simulations mettent en évidence l'importance des procédures claires et de ressources, d'une coordination identifiée et dédiée, de rôles définis et d'une communication maîtrisée, notamment en impliquant la direction générale pour assurer une compréhension globale des enjeux.

> *« Et puis faire passer des messages […]. Le fait de jouer avec la direction générale, on a fait un exercice avec la direction générale, ça a été de leur dire, voilà, il n'y a plus d'IT pendant trois semaines, c'est quoi votre stratégie ? C'est quoi la stratégie du métier ? […]. Mais en fait, c'était ça, les scénarios, c'était de se dire, c'est quoi, on met tout de suite la clé sous la porte ? Parce qu'on ne pourra pas, soit on trouve une stratégie en disant, on délivre nos gros clients. Hypothèse, ou on délivre uniquement les clients qui ont un récurrent, qu'on connaît, qu'on maîtrise. Et puis, on continue comme ça. … Donc, voilà, c'est un peu les remettre devant des situations où se dire, ah oui, ça on n'y avait pas pensé. Effectivement, comment le métier s'adapte ? Parce qu'en fait, la crise cyber, il y a la crise cyber mais il y a derrière toute la partie métier en fait. Et c'est ça qui n'est pas toujours compris. Et qu'il faut faire comprendre. C'est, si je n'ai plus d'IT, comment mon métier fonctionne ? Parce que souvent, nous, c'est de dire, il y a un incident, je ne sais pas, on a perdu, le site est coupé, ça va revenir, il faut attendre d'ici trois heures ou quatre heures. Donc les gens, ils patientent. Ils savent qu'ils vont finir plus tard. Ils savent que ça va être un peu compliqué parce qu'il va falloir rattraper. Mais ils se disent, on attend que l'IT revienne. Mais là, en fait, on ne pourra pas faire revenir l'IT. Donc c'est ça aussi qui est hyper important, c'est de se tester, mais aussi de faire passer tous ces messages-là. »* (Ent.10, logistique)

La sécurisation des systèmes d'information ne repose donc pas uniquement sur la technologie, mais s'appuie sur une organisation et une gouvernance adaptée, prête à tester et améliorer les processus établis. Le développement de plans de gestion de crise cyber, plans de continuité de l'activité ou de reprise d'activité, suppose *a priori* une structuration de la cybersécurité dans l'entreprise avec au moins un poste ou une équipe dédiée ou attachée à des rôles spécifiques « en interne », ce qui n'est pas le cas des plus petites entreprises en dehors du secteur du numérique.

Information, sensibilisation et formation

L'Information et la sensibilisation jouent un rôle essentiel dans la prise de conscience, en présence de pratiques inconsidérées de la part des employés, et pour la sécurisation des systèmes d'information, en particulier face à la résistance rencontrée lors de l'adoption de nouvelles pratiques en cybersécurité. Comme l'indiquent plusieurs entretiens, l'introduction de nouvelles mesures telles que l'authentification forte - d'autant plus si elle implique l'utilisation d'un téléphone personnel pour accéder au SI de son entreprise - ou la restriction des droits d'administrateur pour des développeurs sur leurs postes de travail (vécue comme une limitation dans leur

travail), suscitent des réticences de la part des utilisateurs, qui perçoivent ces changements comme des contraintes supplémentaires.

> « En fait, la MFA, ce n'est pas une technologie, c'est une technique où tous les utilisateurs qui se connectent de l'extérieur du réseau doivent avoir confirmé leur identité via un téléphone. Donc ça, c'est l'authentification à deux facteurs, donc là, au début ça grognait un petit peu parce que du coup tout le monde n'a pas de téléphone pro donc voilà, nous on a dit que si vous voulez vous connectez de l'extérieur, la condition sine qua none, c'est que vous installiez une application d'authentification sur votre téléphone personnel. Sinon, non. Sinon il y a des personnes en télétravail ou il y a des itinérants ou autres du coup, ils ne pouvaient plus accéder au SI. » (Ent.3, agriculture).

Pour les surmonter et favoriser l'acceptation de ces mesures, les enquêtés rapportent que les entreprises, par l'intermédiaire de leur responsable des systèmes d'information, instruisent une communication régulière « pédagogique », pour expliciter les raisons de ces nouvelles pratiques, leur importance pour la protection collective de l'entreprise. La sensibilisation s'appuie sur une communication continue plus ou moins formelle, comprenant, par exemple *« au moindre doute sur le mode de transmission de données »* (par exemple, un changement dans le fonctionnement d'un fournisseur ou d'un client), un recours à une procédure de vérification par téléphone, ou pour les entreprises les plus avancées en la matière, des campagnes d'information avec l'usage d'un Chatbot ou de webinaires de courte durée et à répétition pour la formation des collaborateurs et la sensibilisation au phishing notamment.

> « On avait commencé à le mettre en place il y a un an ou deux ans maintenant, c'est un outil en ligne une sorte de Chatbot sur la formation […], de la sensibilisation avec un Chatbot qui explique voilà c'est quoi un phishing, c'est quoi un hacker, quelles sont leurs méthodes, plein de petites choses comme ça. Et en parallèle de ça, il y a de la sensibilisation avec du faux phishing aléatoire. On envoie des mails qui peuvent être avec la signature [de la direction] ou la signature d'un client […] qui nous demande d'ouvrir la pièce jointe parce qu'il faut aussi signer le contrat rapidement. Donc c'est à nous de faire attention et de relever les indices qu'on a appris pendant les cours et de signaler le mail… Et de là, en fonction du nombre de cours qu'on a complétés et du nombre de mails qu'on a reportés, signalés à la plateforme, on a des points et un classement sur la globalité de l'entreprise. Et un pain au chocolat pour les trois premiers ! » (Ent.5, industrie).

> « On a beaucoup travaillé sur la sensibilisation. On est en train de déployer une plateforme, justement, pour tester et sensibiliser nos utilisateurs, nos collaborateurs. Donc, ça, c'est en cours de déploiement. » (Ent.10, logistique).

Des campagnes de faux phishing sont également confectionnées ; elles sont considérées comme très efficaces par ceux qui les ont instaurées, pour développer progressivement en entreprise une culture collective de la vigilance. *« On sait, mais de le faire, de le mesurer, de le voir en fait et de communiquer autour […] c'est hyper important »*. D'autant plus, avec le développement d'outils d'IA qui peuvent aussi servir la cybercriminalité, comme le déclare un enquêté :

> « On n'en a pas beaucoup parlé mais il y a le côté intelligence artificielle, fake, je peux répliquer la voix. Moi, je sais que j'ai montré à mon DG, je lui ai dit, voilà, regarde j'ai pris une photo de toi que j'ai trouvé, ta voix que j'ai trouvé sur You Tube et je t'ai fait un avatar, et je t'ai fait dire ce que je veux. Et un peu de sensibilisation, ce n'est pas parce que vous entendez la voix de votre DG au téléphone qui, tout d'un coup, vous demande un truc dans l'urgence qu'il faut le faire… Voilà il y a toute une sensibilisation à faire par rapport à ces enjeux-là qui sont hyper importants et qui n'est pas forcément un gros investissement. » (Ent.8, transport et logistique).

Pour les professionnels des métiers de l'informatique interviewés, l'évolution permanente du métier et des technologies implique de faire de la veille, de s'informer sur la sécurité, les contextes de menaces, les techniques et les risques liés à certaines technologies en suivant notamment par abonnement le bulletin publié par l'ANSSI, les bulletins de la DGA, ou certains sites d'informations, ou encore, en participant à des rassemblements et échanges de professionnels du secteur via des clusters régionaux par exemple, ou des forum spécialisés comme celui de la cybersécurité qui relaie les tendances et l'actualité sur le sujet. Cette veille est réalisée particulièrement à partir des outils (bulletins d'actualité – CERT-FR[24], des menaces et des incidents de compromission, des recommandations, des points de contrôle visant à identifier les faiblesses de certains produits technologiques) qui sont mis à disposition par l'ANSSI, *« une entité hyper reconnue en Europe »* souligne un enquêté : *« On a la chance d'avoir avec l'ANSSI beaucoup d'informations »* (Ent.10, logistique) ; ou un autre : *« de toute façon, c'est l'ANSSI, c'est l'agence de sécurité informatique. On a la chance maintenant, on a un pôle à Rennes »*. La veille est donc aussi considérée comme *« quelque chose de primordial »*. Ces outils informationnels

[24] https://www.cert.ssi.gouv.fr/actualite/

(guides des bonnes pratiques ou référentiels) permettent de diffuser efficacement les bonnes pratiques, d'informer sur les risques émergents et les solutions innovantes et de renforcer la culture de la sécurité au sein des entreprises. Par exemple, un acteur évoque la mise en place d'une cartographie de leurs applicatifs, alimentée par des alertes et des échanges avec l'ANSSI, afin de mieux maîtriser leur environnement informatique en cas de découvertes de vulnérabilités (Ent.8, transport et logistique).

Un autre point, relatif à ce volet, concerne le défaut d'informations ou de lisibilité pour la collaboration avec les prestataires. Dans un contexte de recours et de dépendance accrue à des prestataires, la demande de labellisation ou de certification des systèmes apparaît de plus en plus souhaitée. En fonction du développement et de l'accroissement du nombre des technologies mises en place pour la gestion de la prévention et des méthodes de protection des systèmes d'information et aussi de leurs évaluations (audits, tests d'intrusion etc.), le nombre de prestataires auxquels font appel les entreprises a considérablement augmenté. Pour certains acteurs interviewés, hormis la norme ISO 27001 qui édicte des règles bien établies, il n'y a pas de labellisation (Ent.7, industrie), or la certification permettrait d'établir un cadre de référence plus clair et de renforcer la confiance dans la conformité des systèmes de sécurité mis en place. L'entrée en application à partir de décembre 2027 du *Cybersecurity Act* (UE 2019/881) devrait cependant combler cette lacune, puisque cette réglementation européenne s'adresse particulièrement aux fabricants et fournisseurs de produits, services et processus technologiques de l'information et communication pour qui elle fixe un ensemble d'exigences de sécurité.[25]

En résumé : généralement précédée d'une auto-évaluation ou d'un audit externe (test d'intrusion, par exemple), la protection contre les cybermenaces est un processus itératif et se décline en trois pans : technologique et technique (intégration et évaluation d'outils de protection des systèmes d'information), organisationnel (structuration des procédures, de la communication et de la coordination de crise) et informationnel (sensibilisation, communication interne et la veille informationnelle). Toutefois, les aspects organisationnels et de gouvernance (les plus complexes) ne concernent que les plus grandes entreprises enquêtées ou celles du secteur du numérique. Enfin, une plus grande transparence de la part des prestataires est toutefois attendue par les entreprises, ce que devrait permettre le *Cybersecurity Act* (2027).

III. Des contraintes fortes pour les entreprises : Investissements, normes et réglementations

Protéger activement ses données et son réseau impose aux entreprises enquêtées des contraintes fortes en matière d'investissements techniques, d'obligation de conformité aux normes (ex. certifications) et réglementations, de mesure et de contrôles de l'efficacité des investissements réalisés. Ces coûts sont très élevés et les budgets récurrents dans un domaine en perpétuelle évolution technologique. Si les budgets alloués attestent d'« une bonne conscience que la sécurité c'est important, ça a un coût » (Ent.8, transport et logistique), les entretiens témoignent aussi sur l'existence de coûts cachés de la cybersécurité pour une attribution qui peut être connexe à l'activité centrale de l'entreprise mais non à son fondement : temps humain, compétences métier, dépenses et dépendances accrues envers les prestataires, interdépendances des systèmes des technologies de l'information et des systèmes opérationnels… La gestion proactive des risques cyber et la justification continue des investissements, souvent sous contrainte de ressources humaines limitées, restent des axes clés identifiés par les enquêtés, informaticiens, pour améliorer en continu leurs actions de protection et limiter la dette technique à long terme.

Des coûts d'investissements importants et un budget récurrent

« Normalement en cybersécurité on se dit qu'il faut 2 à 5% du CA investi dans la cyber » (Ent.5, industrie)

Les investissements en cybersécurité sont très importants, notamment pour la modernisation et la mise à niveau des infrastructures, qui avaient été sous-investies jusque-là (changement d'opérateur, interconnexion des sites, adoption de technologies avancées telles que la fibre optique, la 4G), la sécurisation des accès (VPN, backups,

[25] https://cyber.gouv.fr/cybersecurity-act

procédures pour nomades ou fournisseurs). Une entreprise du secteur industriel a par exemple récemment changé d'opérateur pour bénéficier d'un niveau de sécurité supérieur, intégrant des outils de filtrage et des procédures de sécurité pour les travailleurs nomades. Ce changement a permis de structurer la communication entre les différents sites de l'entreprise, remplaçant un système chaotique reposant sur une *« multitude d'opérateurs avec des VPN à l'ancienne avec différents opérateurs »* (Ent.7) par une solution unique et sécurisée.

> *« Et on peut même bosser avec notre système, on peut même bosser en étant complètement coupé d'internet. C'est-à-dire qu'on peut bosser en autarcie, on coupe l'Internet, plus personne n'a Internet, mais on peut bosser entre nous. Donc on peut s'isoler si besoin et, si il y a…là, on coupe, ça se fait très facilement. »* (Ent.7, industrie).

Depuis quelques années, certains budgets octroyés à l'*IT* ont donc connu une croissance significative. Des investissements tant technologiques qu'humains, notamment par le recrutement (création de fonction de Responsable de la Sécurité des Systèmes d'Information, Délégué à la Protection des données, …), ont plus que doublé pour certaines entreprises enquêtées, d'autant s'il n'existait pas de poste dédié à plein temps sur la sécurité de l'infrastructure. Pour autant, les plus petites entreprises ne recrutent pas nécessairement en interne ce type de poste, mais peuvent externaliser entièrement la sécurisation de leurs systèmes à un ou des prestataires ou encore s'associer entre PME d'un même groupe pour la déléguer à un prestataire. Si la sécurité ne représente pas forcément le plus gros budget de l'IT, elle connaît désormais une évolution majeure. Le renouvellement des équipements pour une gestion plus fine de l'obsolescence (matériel utilisateur, parcs informatiques récents, interconnexion des sites d'entreprise), l'installation de multiples nouveaux outils logiciels de détection et de protection contre les attaques, l'évaluation systémique des processus d'amélioration, de conformité ou des démarches de certification, par des audits interne et externe et des tests opérationnels nécessitant à chaque étape du process un accompagnement par des experts spécialisés ou une équipe de soutien, avec un nombre toujours plus importants de prestataires. Les investissements requis en matière de cybersécurité ne se limitent donc pas non plus à l'infrastructure. Les logiciels de sécurité par exemple sont désormais souvent proposés sous forme d'abonnement payés mensuellement par utilisateur, ce qui peut rapidement faire grimper les coûts.

> « Il y a le coût, un facteur qui devient problématique, on l'a vu depuis deux ans, c'est le fait que nous, quasiment tous les éditeurs, ils ont maintenant un problème de solution face […]. C'est des abonnements » (Ent.9, numérique et santé).

« Il faut donc avoir le budget pour pouvoir mener tous les projets » (Ent.10, logistique). Il y a donc une évaluation du coût.

> *« Il y a une évaluation coût, c'est-à-dire le delta annuel qui est là. Généralement, c'est les modulos ou du Syntec qui font que les contrats évoluent. Il y a des fois où c'est un éditeur qui dit qu'on passe du mode maintenance classique à un mode locatif. Là on multiplie par 7 le coût annuel donc là on réfléchit à deux fois alors c'est quand même le coût et puis si vous avez, je vais être clair… Si vous n'avez pas eu d'enmerdement pendant un an, deux ans avec un prestataire et puis qu'à chaque fois qu'il y a eu un truc, il a répondu, il a eu la réponse technique. Vous ne cherchez pas, vous avez d'autres chats à fouetter que de chercher, sauf si on a des bruits de couloir en disant attention la techno est en train de tomber, le prestataire c'est plus la même équipe et ainsi de suite… Là on est vigilant mais sinon à partir du moment où on a une techno en place qui fait le job, sauf si on a des recommandations mais je vous dis, ce programme-là, je n'allais pas dire que c'est notre vecteur, mais c'est un très bon support. »* (Ent.7, industrie).

Les investissements sont priorisés par les entreprises dans une démarche, scandée par des étapes mais, inscrite sur le long terme et *« jamais terminée »*, y compris par exemple la certification ISO 27001 qui doit être renouvelée tous les trois ans, contrôlée tous les ans et qui connaît des versions successives (par exemple *« la 2022 »* qui ajoute l'installation d'un SIEM).

> « En fait, l'investissement est tellement colossal qu'on ne pouvait pas tout faire. On ne peut pas partir de zéro et arriver à 100 sur une année. En termes budgétaires, même moi j'ai pas de problème pour valider les budgets de sécurité auprès de mon DG […]. Donc déjà budgétairement c'est assez colossal parce que ça ne dégage pas de valeur, il ne faut pas l'oublier ! » (Ent.3, agriculture)

Plutôt que de l'aborder sous l'angle de la priorisation, certains posent le problème à l'envers, précisant qu'« *il y a des systèmes qu'on a un peu laissés de côté, et qu'on est en train d'attaquer là, cette année »* (Ent.3), faisant référence directement au futur chantier de sécurisation de l'informatique de système industriel (OTI), après avoir bien engagé la sécurisation de la protection du système d'information de gestion. Deux systèmes qui ont été rendu en quelque sorte étanches, *« mais malgré tout, il y a des connexions »* (Ent.3, agriculture). Des montants

de dépenses jugés toujours très élevés (des milliers d'euros) en fonction de l'échelle de l'entreprise *(« est-ce qu'une petite structure peut faire ça ? »*).

Les coûts peuvent aussi être très variables, selon qu'il y a ou non un accompagnement derrière ou selon que l'on est dépendant techniquement. Par exemple, la mise en place de la DLP ou *Data Loss Prevention*, une mesure de sécurité stratégique qui garantit que les informations sensibles ou critiques ne sont pas transmises en dehors du réseau de l'organisation. Ces mesures comprennent des outils et des logiciels qui permettent un contrôle administratif des données. Selon un enquêté, cela peut être envisageable d'installer de la DLP pour une entreprise de petite taille mais si elle est du secteur du numérique : « *Alors nous, ça va, parce que c'est une boîte d'infos machin, mais dans une petite structure de 10 ou 20 personnes qui ne fait pas plus d'info, ça commence à coûter cher. »* (Ent.9, numérique et santé)

> « C'est quand même à chaque fois c'est des logiciels où le ticket d'entrée c'est 20-30000 euros. […]. C'est surtout… Il faut énormément de monde et ça coûte extrêmement cher. […] et techniquement c'est compliqué. » (Ent.9)

Les coûts technologiques sont donc aussi associés à des coûts humains croissants, non seulement en termes de compétences nécessaires face à l'augmentation de la complexité technique, mais aussi de temps de travail et de charge de travail « *des équipes derrières qui prennent en compte tous ces aspects-là »* (Ent.10, logistique) ou du recours accru à de nombreux prestataires, pouvant aller jusqu'à plus d'une centaine pour une seule entreprise pourtant de taille moyenne (70 salariés), mais dont les exigences et demandes de la réglementation sont très fortes (Ent.9, numérique et santé).

> « Le gros poste budgétaire, c'est la partie technologique. Donc pour moi, ce n'est pas spécialement la mise en conformité, mais c'est plus l'outil derrière qu'il faudra déployer. Donc ça, c'est un gros poste. Il y a certaines solutions, c'est plusieurs milliers d'euros tous les ans. C'est vraiment des coûts assez conséquents. Je pense que les temps humains aussi. Et puis, comme je dis, on demande de plus en plus de choses en termes de cybersécurité auprès des équipes. Mais en fait, les équipes, elles n'ont pas que ça à faire. Elles font tous les projets, le run. Et en fait, il y a un coût humain aussi important. Et ça, on a du mal à… cette charge, on a du mal à la faire absorber par les équipes. » (Ent.10).

La mise en place des mesures de protection cyber se traduit par un surcroît de travail qui repose sur les équipes techniques pour *« faire appliquer les mesures »*, dans une entreprise où par exemple les ressources humaines dédiées sont trop faibles, comme le rapporte cet enquêté d'une entreprise de plus de 20000 salariés, localisée dans sept pays européens, où ils ne sont que *« deux et demi pour toutes les AP »* (Ent.10).

> « Mieux cadrer et essayer de préparer les équipes. Enfin, là, il y a un bout de travail. Et je ne vous cache pas, c'est le manque de bras qui fait qu'on ne va pas à la vitesse que l'on souhaiterait. » ((Ent.10, logistique).

> « Moi, ma projection c'est de me dire, il y a des risques, il va falloir que l'équipe grossisse. Il y a des sujets techniques. Il y a beaucoup de sujets techniques. Et je pense qu'il va falloir que certaines personnes gèrent cette partie un peu technique. Et il va falloir continuer à prendre de la hauteur. Je pense que c'est ça, un peu, une de nos problématiques. A deux et demi, ce n'est pas simple. Mais prendre un peu de la hauteur et pouvoir mieux piloter les risques et tout ce qui est remédiation et pilotage global de la cyber. » (Ent.10, logistique)

Malgré l'importance croissante de la cybersécurité, les enquêtés rendent compte de freins budgétaires. Et quand il n'y a pas de débats sur ces questions-là au sein de l'entreprise au sens où la plupart des investissements en cybersécurité sont acceptés par leurs directions, il s'agit *« de ne pas faire non plus exploser les budgets »* (Ent.9, numérique et santé). Les discussions autour des budgets peuvent cependant aboutir à des arbitrages difficiles, où la sécurité en dépit d'*« un investissement chronique »* (Ent.8, transport et logistique) est surtout perçue comme un coût *« pour quelque chose qui ne dégage pas de valeur »* (Ent.3, agriculture), plutôt qu'un investissement. Un des enquêtés décrit, à partir de l'exemple de la mise en place d'un SOC, qui avait été dépriorisée *« avec l'idée d'attendre un peu avant d'investir davantage »*, ce phénomène qu'il analyse comme *« le syndrome du jusqu'ici tout va bien »* (Ent.8, transport et logistique). Ce qu'il considère comme un risque non négligeable. Les tentations de réduction ou de report des budgets existent, particulièrement pour les entreprises dont l'IT est davantage une fonction support et que la cybersécurité est définie par ces entreprises comme connexe, voire annexe, à leur activité, alors que la nécessité de se protéger contre les menaces croissantes devrait, selon eux, pousser à maintenir, voire augmenter ces investissements pour *« prendre de la hauteur »* (Ent.10), sans accumuler de la dette technique avec des systèmes non conformes à la réglementation.

Parmi les investissements réalisés, la souscription d'une assurance cyber n'a été contractualisée que par cinq entreprises parmi les onze enquêtées (soit près de la moitié). Deux d'entre elles, issues du secteur de la logistique, sont aussi les plus importantes en taille. La troisième entreprise qui a souscrit une assurance cyber depuis des années est soumise à de nombreuses demandes de réglementations qui sont très fortes, eu égard à son double secteur d'activité (numérique et santé) ainsi qu'aux réglementations imposées à leurs clients et aux contrôles que leurs clients leur imposent tous les ans. Si l'assurance cyber n'est pas requise pour la certification ISO 27001, cette entreprise l'avait prise dans la même période d'engagement dans cette démarche. Les assurances cyber scannent l'exposition de l'entreprise aux risques et obligent à des actions de modernisation, de mise à niveau ou de correction de failles par exemple. Cette surveillance de l'état du SI exige des actions en retour. A défaut de procéder aux modifications nécessaires, les assureurs cyber refusent de couvrir certains risques. Les motivations à la contractualisation de ces assurances spécifiques sont donc à trouver par exemple dans l'évaluation et l'accompagnement qu'elles fournissent pour *« rentrer dans la charte »* (Ent.8), dans une temporalité définie. Mais l'argument le plus fort renvoie à l'assistance technique d'experts intervenant en quelques heures, ce dont les contractants de l'assurance cyber bénéficient en cas d'attaque : *« les pompiers cyber »*.

> « On a aussi adossé une… Donc c'est un peu une assurance technique, mais on a un contrat avec CSIRT[26]. Donc en cas d'événement cyber, on peut les contacter et ils interviennent en quatre heures. Entre guillemets, on appelle ça, nous, les pompiers cyber. » (Ent.10). « Ils interviennent en quatre heures pour nous accompagner à identifier et à prendre les mesures adéquates pour se mettre en protection […] et pour identifier l'origine de l'attaque. » (Ent.10, logistique)

> « On l'a surtout pris en cas d'attaque de ransomware pour bénéficier d'une assistance technique d'experts pour permettre… l'identification du chemin d'attaque. Après, parce que… la perte exploitable, la perte d'exploitation il n'y en aura pas. […]. Le vol de données… Après on n'est pas responsable de traitement. Donc la vente, ce sera plutôt chez le client. Donc, la perte d'exploitation aussi. […] Ca va surtout être de l'expertise technique qui va nous coûter cher. Pour moi c'est ça. […]. Notre risque principal c'est vraiment un manque d'expertise technique qu'il y a d'être cyber-attaqué. » (Ent.9).

Les autres enquêtés justifient d'un « volet cyber » dans la responsabilité professionnelle du contrat d'assurance, sans davantage en connaître précisément les conditions. La démarche d'assurance cyber également très coûteuse incite donc également les entreprises à la mise à niveau des systèmes pour satisfaire aux exigences des assureurs.

Dans un contexte de priorisation sur d'autres investissements plus au cœur de l'activité de l'entreprise, la difficulté à obtenir des budgets suffisants pour la cybersécurité, est un risque qui peut en effet freiner la mise en œuvre des mesures. Seul un enquêté, dont la direction est partie prenante de clusters régionaux où les informations circulent, parmi les onze entreprises répondantes, évoque un soutien financier obtenu dans le cadre d'un programme industriel (France-Relance), qui a permis notamment la création de la fonction SI au sein de son entreprise, et la mise en place d'un système d'information plus robuste (Ent.7) *: « et dès qu'il y a une aide, il y a un projet […]. Donc il y a des aides et dès qu'on peut avoir des aides, on y va ! »*. Le manque d'informations, la faible identification de supports financiers existants ressort très nettement de cette enquête.

Des normes et contraintes réglementaires… d'autant plus fortes selon les secteurs

Principalement conçue pour renforcer le dispositif de cybersécurité des fournisseurs de services essentiels, rationaliser la cyber-résilience grâce à des exigences et à une application plus stricte et des sanctions en cas de non-conformité, ou encore améliorer la préparation aux cyberattaques en imposant des pratiques communes par exemple de signalement des incidents et le partage des informations qui jouent un rôle dans la prévention et la détection des dangers, la directive européenne NIS 2 (*Network and Information System Security* 2)[27] s'applique particulièrement aux secteurs de l'énergie, des transports, de la santé, de la banque, de l'eau potable, des services numériques, des administrations publiques et autres secteurs clés. Les opérateurs de services essentiels ou les fournisseurs de services numériques, englobés avec NIS2 dans la catégorie juridique « entités essentielles ou importantes », sont singulièrement visés.[28] Pour les prestataires, en effet, les réglementations

[26] Les réseaux CSIRT – CERT-FR, https://www.cert.ssi.gouv.fr/csirt/

[27] NIS 2 (entités essentielles et importantes) mais également la directive REC (entités critiques)

[28] Avec NIS 2 on ne parle plus d'OSE et de FSN (NIS 1) mais d'entités essentielles et importantes. Dans cette étude empirique, nous avons fait le choix de conserver la terminologie issue du terrain d'enquête et toujours active et mobilisée par les acteurs concernés au moment où l'enquête a été réalisée.

s'appliquent indirectement via des contrats et aussi de nouvelles réglementations spécifiques comme le CRA, règlement sur la cyberrésilience. Parmi les entreprises enquêtées, toutes sont touchées par cette réglementation, soit directement selon leur taille et/ou secteur d'activité, soit indirectement dès lors qu'elles font partie de la *supply chain* d'entreprises de secteurs critiques, comme l'observe un enquêté dont l'entreprise produit principalement de l'usinage série pour l'aéronautique et la défense.

> « On est concerné indirectement, parce que comme on est supply chain de domaines où c'est obligatoire […]. Le NIS 2, c'est une histoire de taille d'entreprise, mais aussi une histoire de domaine. Si vous êtes du domaine, de toute façon, que vous soyez 1,10,20 ou 30 vous êtes obligés d'y passer parce que là, c'est figé, et on va y avoir droit indirectement. […]. On s'y prépare et on commence à regarder ce qu'il faut mettre en place ». (Ent.7, industrie).

La démarche de certification ISO 27001, engagée par exemple par deux entreprises enquêtées (Ent.9, Ent.2), valide les récentes et nouvelles réglementations.

> « Là, ça va être directement. DORA pas directement, parce qu'on n'est pas une entité financière, mais c'est nos clients. Par contre oui NIS 2 on est dessus direct. Par contre vu le projet de loi, quand on est certifié 27001, ça ne va pas changer des milles et des cents. C'est du genre, j'ai vu ce qu'ils ont sorti. Voilà pour moi, à part la déclaration d'incident à l'ANSSI grosso modo, il n'y a pas de changement. […], toutes les mesures de sécurité, elles sont déjà en place ». (Ent.9, numérique et santé)

Mais selon la spécificité du secteur d'activité, des réglementations auxquelles sont soumises les clients (des entreprises) des entreprises, d'autres réglementations ou procédures de normalisation ou de contrôles peuvent s'imposer par répercussion.

> « On a des certifications. C'est normal, mais tous nos clients, ils sont soumis à une réglementation de la CPR[29] et on a des contrôles de leurs commissaires aux comptes tous les ans. Voilà, donc au début, il y a quelques années, il n'y avait pas ces contrôles IT, ça a été vachement augmenté et ça devient très chronophage. » (Ent.9).

> « C'est logique… parce qu'il y a eu, il y a donc leur autorité de contrôle qui s'est emparée du sujet. Il y a la réglementation européenne DORA, là, qui, en œuvre depuis le 17 janvier, mais avant, la CPR demandait quand même des choses. Et, bon après, voilà, nos clients, c'est considéré comme des entités financières, donc ils sont soumis aux mêmes règles que oui, c'est-à-dire que les banques, alors, un peu light pour certaines, mais dans l'esprit ça reste le même règlement, donc ça reste des trucs pour la taille de leur structure, ça reste lourd. » (Ent.9).

Cette dépendance à des tierces et l'exigence de contrôles réguliers rendent notamment la gestion des sous-traitants critique et d'autant plus coûteuse et chronophage.

> « En fait, c'est les demandes de la réglementation qui sont fortes. Elles sont fortes. Le cas simple, là, il demandait pour la semaine prochaine. Donc ils nous ont dit en janvier, fin janvier qu'ils voulaient le fichier des sous-traitants, de nos sous-traitants, des mutuelles, des sous-traitants des mutuelles et des sous-traitants des sous-traitants et les sous-traitants des sous-traitants des sous-traitants. Un truc de fou. Donc, il fallait fournir ça. On va dire à la CPR dans un format à la con, où il y a plein d'infos pas si simples que ça à récupérer sur les sous-traitants… Des sous-traitants, on en a plein. Des sous-traitants il y en a… Des sous-traitants qu'on a défini comme sous-traitants pour l'activité, on en a une centaine. Donc, rien que récupérer leur code EID machin, aller sur les sites […], récupérer ça, ça prend un temps fou. Donc il n'y a rien d'automatisable. Tout doit être fait à la main. Tout est long. Tout, et c'est horriblement long. Donc, pour une mutuelle c'est ultra chronophage. En plus, on a un temps assez court. Finalement, un temps assez court. Sachant qu'on a des problèmes bassement informatiques, genre le format du fichier, qui est loin d'être facile à remplir. Et avec plein de contrôles. […]. L'Europe, c'est beaucoup de normes compliquées et pas beaucoup d'aides. » (Ent.9).

Certaines règles apparaissent si complexes à mettre en œuvre, notamment en matière de protection des données sensibles, que selon un enquêté, elles ne pourront pas l'être. Par exemple, l'impossibilité dans le domaine de la santé d'envoyer un mail avec des données et l'identification de la personne. Seuls les médecins ont un système de messagerie sécurisée pour la transmission de ces données entre eux.

> « Nous, par exemple, on n'a pas accès à ça. Si on veut écrire à un médecin, on ne peut pas utiliser ce système de messagerie. Donc des fois on ne peut même pas leur envoyer un mail tout simplement parce que c'est refusé automatiquement par leur système

[29] Caisse de prévoyance et de retraite.

> et dans leur système, c'est pour ça que dans les courriers des médecins en général on met juste un prénom on ne va pas mettre le nom de famille […]. » (Ent.6, santé)

Cette obligation réglementaire à laquelle s'ajoute l'absence de système de transmission existant pour leur métier leur imposerait une gestion de mails séparés, ce qui opérationnellement est lourd au quotidien, *« à moins d'imaginer un système de chiffrement de toutes nos données internes et que nos logiciels puissent ouvrir ces données, les décrypter. Là déjà, ça va au-delà de ce qu'on peut faire puisqu'on n'a pas la maîtrise de l'outil. »* (Ent.6, santé).

Les normes et les réglementations permettent d'abord de confronter la gestion de la cybersécurité mise en place : « *si la roadmap est conforme à toutes ces exigences »* (Ent.10, logistique). Elles obligent *« à voir, à vérifier que le système de management de la sécurité est efficient »* (Ent.9, numérique et santé). Mais elles contribuent également, ensuite, à appuyer et conforter la démarche proactive des équipes investies *« qui ont une bonne vision »*, qui par ses actions a anticipé le respect des normes, justifiant ainsi *« des stratégies judicieuses puisqu'on s'aperçoit qu'il n'y a pas un investissement massif à mettre en œuvre, c'est juste une continuité »* (Ent.10).

> « Parce que typiquement le SOC, ça fait trois ans qu'on l'a mis en place. Mais c'est vrai que quand on dit à la direction générale, vis-à-vis de la conformité de NIS2, ça fait trois ans qu'on l'a mis en place. […]. Donc la conformité NIS2, cette partie-là, nous, on l'a déjà adressée. […], je ne vais pas dire que le NIS2 est un non-événement, ce n'est pas vrai, il y a encore plein de choses à faire, mais il y a beaucoup de choses qui permettent de dire, regardez, dans notre stratégie qu'on a menés depuis plusieurs années, quand on regarde aujourd'hui les exigences que l'ANSSI va nous donner, entre guillemets, on a déjà coché un certain nombre de cases. » (Ent.10, logistique).

Cette légitimation de la stratégie des équipes par les normes renforce les choix qui ont été faits, ce qui permet aussi de défendre et motiver les futures décisions budgétaires en la matière, y compris pour des projets onéreux.

> « Donc notre stratégie est bonne. Et donc, quand on va vous demander un budget pour ceci ou pour cela, ça va aussi dans le cadre de renforcer notre sécurité cyber et d'être conforme aux exigences européennes. » (Ent.10)

Avoir anticipé le suivi des cadres réglementaires peut donc permettre de valider une « stratégie cyber » et de justifier des investissements auprès de la direction pour maintenir la « continuité », notamment vers ce qui constitue pour cette entreprise engagée dans une démarche de certification ISO 27001 pour l'hébergement de données mais aussi pour le développement de code et d'applicatifs : *« une évolution naturelle de l'hébergement et du développement », « il faut inclure ces process-là »* (Ent.2).

La mesure de l'efficacité des investissements réalisés

La mise en place d'indicateurs précis de la mesure de l'efficacité des investissements est en cours, mais encore incomplète ou en développement, souvent à peine amorcée, pour les entreprises enquêtées, même si l'efficacité des investissements a déjà pu être constatée par l'arrêt d'attaques grâce aux systèmes qui ont été installés ou encore la sensibilisation des collaborateurs.

La mesure de cette efficacité se fait principalement via les audits interne et externe, des exercices réguliers ou des tests d'intrusion, de simulations d'attaques. Ils vérifient la capacité en chaîne de détection et de réaction.

> « En fait, on a mené il y a trois ans un exercice de type Red Team. […]. C'est une prestation où on prend un prestataire donc, c'est une espèce d'auditeur « Pen tester ». On ne prévient personne. […] Et on lui dit, cotre objectif, votre mission donc, on vous donne X jours. Et votre mission c'est d'atteindre ces trois objectifs. Donc, vous vous débrouillez. Vous passez par la porte, par la fenêtre. Vos objectifs c'est ça. Prouvez-moi si on est vulnérable ou pas. Donc en fait, les gens interviennent et font le… donc, ça permet de déceler des chemins qu'on n'aurait pas pu identifier. Ça permet aussi de vérifier la chaîne de supervision. Typiquement, la première fois, moi, j'ai les équipe Active Directory qui m'ont dit « c'est bizarre on a du scan sur tel protocole, ce n'est pas normal. » « Ça permet de vérifier si le SOC détecte aussi des événements suspects. Donc ça permet de vérifier toute cette chaîne. Et justement, de trouver des chemins d'attaque pouvant compromettre notre système d'information. Et donc, ça c'est quelque chose qu'on a fait et qu'on a remonté à la direction générale. Donc là aussi, c'est hyper important parce que c'est visible. » (Ent.10).

Certains projets ou plan de remédiation sont réalisés à la suite de ces audits, perçus comme techniquement intéressants bien que très coûteux. Leur intérêt consiste aussi à montrer et évaluer le niveau de maturité cyber

pour le soumettre à la direction. La mesure de l'efficacité des investissements réalisés fournit une vision de l'évolution. En ce sens, elle regarde spécifiquement la direction des entreprises :

> « Et donc la direction attend le prochain test pour voir justement l'évolution. Est-ce qu'on a amélioré notre posture ? est-ce qu'on est resté à un niveau équivalent ? Ou est-ce qu'on s'est dégradé ? Donc, c'est aussi ça qui les intéresse. » (Ent.10).

Ils permettent de faire remonter beaucoup d'indicateurs, notamment pour mieux gérer l'obsolescence programmée, pour essayer de rattraper le retard ou éviter la dette technique par exemple, mais surtout d'anticiper les besoins ou les contraintes (ex. la migration vers le prochain Windows Server), prévoir les investissements à venir. Par conséquent, ces mesures introduisent un *« changement de posture »* : *« c'est de se dire, maintenant, il faut qu'on essaye d'anticiper et de ne pas courir après le train »* (Ent.10, logistique).

En résumé : les investissements et dépenses technologiques et humains en matière de prévention du risque cyber sont très importants, alourdis par le recours aux prestataires toujours plus nombreux, et ne sont pas toujours prioritaires. Parallèlement, les entreprises et plus singulièrement les prestataires sont soumis à un nombre croissant de normes et réglementations plus ou moins contraignantes selon le secteur d'activités, parfois perçues comme trop complexes. Ces dernières contribuent néanmoins à interroger l'action de l'entreprise en matière de cybersécurité, voire à la valider et à en justifier les investissements. Des audits internes ou externes sont mis en place pour mesurer l'efficacité de l'action cyber et évaluer le niveau de maturité cyber de l'entreprise.

IV. Un impact (ou non) sur la stratégie des entreprises

La prise de conscience croissante du risque cyber, associée aux obligations réglementaires et à la mise en place de mesures de prévention et de méthodes de protection des systèmes d'information par les entreprises particulièrement aux niveaux technologique et technique, ont conduit à une structuration de la cybersécurité au sein des entreprises. Une seule entreprise, de 40 salariés, dans le secteur de la santé, parmi les onze enquêtées, délègue entièrement la gestion de la protection de son système informatique et de ses données à un prestataire informaticien *« pour toute l'infrastructure et le réseau »* (Ent.6), insistant d'un côté sur le coût que représente la sécurité mais rappelant d'un autre côté des obstacles propres à un logiciel métier qui n'évolue plus et qu'ils ne peuvent pas faire évoluer en ce sens *« parce que les solutions de rechange n'existent pas ».* Depuis 4 à 7 ans environ, des entreprises ont commencé à réaliser que leur infrastructure informatique ne pouvait plus soutenir leurs ambitions commerciales notamment, ce qui les a conduits à entrer pour certaines dans des programmes de transformation digitale avec des créations de poste (Ent.5, Ent.8, Ent.3), où la cybersécurité a été intégrée comme pilier du projet, comme le rapporte un enquêté responsable SI d'une PME du secteur industriel :

> « Alors, moi je suis rentré dans le groupe […], voilà, moi je suis rentré le 1er mars 2021 et ils ont commencé à travailler, ce groupement Boost Aerospace a été initié de mémoire pendant le Covid, donc 2019-2020. En fait, nous, notre démarche cyber, alors moi j'ai été embauché dans le cadre d'un appel à projet dans le cadre de France Relance, où en fait on avait ce projet 4.0 donc de mise en conformité cyber de mettre en place un MES donc un logiciel de suite de production en temps réel dans le cadre de ce projet-là, le programme Industrie du Futur, donc on a été France Relance, le programme France Relance, donc on a une aide assez conséquente. Mais en face, il y avait une création d'emploi. La création d'emploi, c'était moi, puisqu'il n'y avait pas de service informatique au niveau du groupe. Il n'y avait pas de service informatique. Et donc ce challenge de création de ce 4.0, il y avait cet outil de suivi de… déjà d'homogénéisation de tous les logiciels, le suivi MES de la production et tout le volet cybersécurité. » (Ent.7).

Pour d'autres, elle a donné lieu à la création d'au moins un poste dédié à la sécurité du SI (Ent.4, Ent.3, Ent.10), voire une équipe liée à la sécurité *« spécialisée autour de la cyber, autour de notre RSSI »* (Ent.8). Sans oublier de surcroît, les très nombreux prestataires auxquels les entreprises ont de plus en plus recours. Ce changement est particulièrement visible dans les entreprises qui ont subi un sous-investissement dans ce domaine, impactant potentiellement leur capacité à innover ou à répondre aux exigences non seulement du marché, mais aussi réglementaires en matière de protection des données personnelles par exemple.

Face à l'ampleur des investissements et du travail requis pour la normalisation et mise en conformité des systèmes d'information, le manque de ressources humaines est souvent cité comme un obstacle à la mise en œuvre efficace des politiques de cybersécurité. Les équipes, souvent réduites, doivent de plus jongler entre les tâches chronophages du contrôle, les exigences opérationnelles et leurs projets au quotidien. Tout ceci peut

ralentir leur activité, mais également la gestion des risques et la mise en place des mesures de protection. Les entreprises doivent donc envisager d'augmenter davantage leurs effectifs pour mieux gérer les sujets techniques pour *« mieux piloter les risques »* et les enjeux stratégiques globaux liés à la cybersécurité.

> « il faut vraiment qu'on prenne de la hauteur, mais je pense que ça, on va pouvoir le faire quand on aura atteint un certain niveau dans l'équipe SSI. […]. Pour moi, il faut qu'on staff encore et pour pouvoir justement avoir des équipes plus sur l'OTI, des équipes plus peut-être sur la partie développement, des équipes plus en charge du SOC, pour que à quelques-uns, on soit plus en mode contrôle, enfin gouvernance. » « Pour moi, ça ne serait pas absurde quand on voit la taille du groupe de passer d'ici quelques années à une dizaine de personnes. Là je pense qu'on est… On a passé un cap. Il faut vraiment qu'on prenne le virage. Je pense que c'est un peu ce que la direction a en tête. Comme je vous le disais on a des postes à pourvoir pour cette année. Un poste à pourvoir. Donc je pense qu'ils ont bien ça en tête. Mais ça va prendre un peu de temps. Mais voilà. Moi, la stratégie, c'est vraiment ça, c'est que la cyber, ça se décompose en différents piliers et il va falloir qu'on mette des acteurs sur chaque pilier pour être beaucoup plus efficace. » (Ent.10, logistique)

> « Alors, c'est plus à mon poste où ça a changé. Il n'y avait pas de RSSI, il n'y avait pas de bras droit. Donc mon bras droit, il est arrivé l'année dernière par exemple. […]. Parce que j'avais tellement de contrôles. J'avais tellement de contrôles à passer que j'étais sous l'eau. On est passé d'un plan de contrôle où il y avait, je ne sais pas 20-30 fiches il y a deux ans. Là on est à 120 fiches de contrôle. Donc, ça n'a plus rien à voir. Après on a été chercher d'autres normes en plus. Donc cette année, on est passé à l'HDS. […]. Il y a une nouvelle version de la certification HDS, la V2. Donc finalement c'est la 27001, 2022. […] Il fallait avoir plus, d'exigences réglementaires de souveraineté, mais qui, pour nous, ne posent aucun problème puisqu'on est franco-français, on a tout en France, on ne travaille pas avec des boîtes extra-européennes. Pour nous, c'est une formalité. Voilà, c'était plus de l'écriture de contrats. Bon il y a des spécificités à mettre dans les contrats. Il y avait pas mal de réécriture de contrats. Techniquement, ce n'est pas un problème. » (Ent.9, numérique et santé)

La structuration de la cybersécurité dans les entreprises enquêtées atteste bien d'un impact sur la stratégie des entreprises, avec des postes en augmentation même si les effectifs en interne restent plutôt faibles face aux défis auxquels les entreprises sont confrontées, tels que la sécurisation à venir de l'*OTI* (informatique des systèmes industriels) pour les secteurs industriel, logistique, agroalimentaire, ou agricole par exemple, ou encore la démultiplication des contrôles, des normes et des certifications pour cette entreprise du double secteur critique du numérique et de la santé (Ent.9). L'exemple de la création d'un poste d'expert en cybersécurité inter-entreprises bretonnes du secteur de l'agriculture et de l'agroalimentaire est un exemple pertinent d'un investissement stratégique, tel que le décrit un enquêté d'une coopérative agricole déjà dotée d'un service d'infrastructure informatique composée d'une direction SI et d'une équipe de dix personnes.

> « Après nous, à notre échelle, on est en train de s'allier avec d'autres entreprises bretonnes pour partager et avoir un expert en cybersécurité bien capé en salarié à temps partagés, porté par du portage salarial, qui pourrait venir tous les mois chez nous, faire un audit des bonnes pratiques avec un œil extérieur » (Ent.3, agriculture).

La volonté de recruter un salarié à très haut niveau de compétences en cybersécurité démontre l'intégration des enjeux de la cybersécurité dans la gouvernance et le besoin d'un accompagnement supplémentaire pointu *« pour apporter des bonnes pratiques, évaluer, tester, nous tenir au courant aussi »,* dans un contexte entrepreneurial où il y a encore toute une organisation à mettre en place (évaluation des systèmes mis en place par des tests, indicateurs d'efficacité, mise en conformité NIS 2, sécurisation de l'*OTI*), malgré des investissements déjà importants réalisés depuis dix-huit mois et qui se poursuivront (Ent.3)

> « On est sur des profils ex-militaires, gendarmes, haute expertise en cybersécurité, donc des profils assez hauts qu'on ne pourrait pas recruter nous à notre échelle, surtout qu'on n'en aurait pas besoin à 100% » (Ent.3).

Des attentes ou des exigences des clients et fournisseurs dans la définition de la politique de cybersécurité

Le deuxième angle fort montrant tout l'impact de la cybersécurité dans la gouvernance et la stratégie des entreprises enquêtées est celui relatif aux attentes et aux impératifs de leurs clients. Les entreprises enquêtées s'adaptent à des normes de sécurité de plus en plus strictes venues de leur marché et entreprises clientes, spécifiquement par exemple dans des secteurs critiques de l'aéronautique et la défense, du numérique et de l'hébergement de données, ou des secteurs sensibles comme celui de la santé. Elles répondent en effet à des exigences fortement orientées par leurs donneurs d'ordre, par exemple par l'intermédiaire d'un programme *« lancé pour justement faire progresser les entreprises du secteur sur cette question de la cybersécurité »*, comme l'indique un enquêté d'une industrie (Ent.5).

> « En fait, c'est une exigence. Enfin, c'est une exigence. C'est ce consortium […], c'est en fait un regroupement actuellement ont est 280 membres de mémoire qui font partie de la *supply chain* de ces donneurs d'ordre. […]. Et donc ce programme-là, il y a un cinquième élément qui est sous-jacent en fait derrière ces quatre donneurs d'ordre, c'est la DGA. […], qui en fait […] supervise un peu tout ce côté sécurité de l'information. Et d'ailleurs à terme moi je suis persuadé qu'ils viendront officiellement apparaître dans les logos, surtout dans le contexte actuel faut pas se leurrer. En fait ce modèle puisque c'est une espèce de corps modèle de veille techno et de suivi techno cyber, d'autres domaines que l'aéronautique commencent à taper à la porte, c'est tout ce qui est de l'automobile, parce qu'eux aussi dans le cadre de la *supply chain* ils ont aussi des exigences de sécurité de fiabilité de l'information et en fait plutôt que de monter un peu leur truc dans leur coin ils se posent la question de venir taper à la porte « vous avez un truc qui a l'air un peu robuste […]» (Ent.7, industrie).

Plusieurs entreprises enquêtées soulignent devoir faire face à des questionnaires intrusifs de la part de leurs clients, qui cherchent à évaluer leur niveau de sécurité. Ces questionnaires, souvent très proches, témoignent d'une volonté de s'assurer que les partenaires respectent des normes suffisamment élevées et en conformité réglementaire. Une entreprise de solutions numériques et d'hébergement entrée dans la démarche de la certification ISO 27001 qui assure *« qu'*[elle] *traite correctement les aspects de sécurité, que ce soit en termes de développement et d'hébergement »* confirme un alignement de la gouvernance de l'entreprise avec les attentes *« des clients qui* [leur] *imposent de plus en plus de choses en termes de contraintes et des niveaux qu'ils exigent »* : *« ça devient très important la 27001 pour les hébergeurs maintenant »* (Ent.2). Ce sont typiquement les *« gros clients qui s'intéressent à ça »*, *« généralement, effectivement, des Enedis, des EDF »*. Ces questions de sécurité deviennent incontournables non seulement du point de vue de la conformité réglementaire mais aussi par répercussion : *« c'est obligé […], c'est surtout ça, nos clients, chefs de projet côté Enedis on leur impose des niveaux plus élevés. Voilà, et ils reviennent vers nous. »* (Ent.2). Ainsi, pour cette entreprise du numérique, si la cybersécurité prend une place un peu plus importante désormais dans les décisions stratégiques, c'est davantage *« par vocation »* que des investissements sont faits, plus que par priorisation. L'intégration de la cybersécurité dans la stratégie de l'entreprise est *« une évolution naturelle de l'hébergement et du développement »* (Ent.2). Elle fait désormais partie intégrante du développement (*« Secure by design »*) et de l'hébergement. Le même argument est développé par un enquêté, Responsable de la sécurité du SI et délégué à la protection des données (DPO), au sein de son entreprise du secteur du numérique et santé (Ent.9). Pour lui, il ne s'agit pas de priorisation : *« des logiciels ont été rajoutés au fil du temps, à la fois parce que c'était une demande du marché, que… voilà, ça devient une brique indispensable »*, et il ajoute : *« on est obligé d'y passer »*. Les attentes de leurs clients sont réfléchies essentiellement par leur tutelle qui a un niveau d'attente très élevé, puisqu'un incident de sécurité par exemple de disponibilité de deux heures doit être déclaré à la tutelle : *« il y a une grande demande du législateur d'avoir des remontées sur des incidents en cybersécurité ».* La conformité et la cybersécurité sont prises en compte dans la stratégie de son entreprise : *« c'est l'argument de fond numéro un »*, car *« la première chose qu'un client va demander, c'est ça, c'est la conformité à DORA*[30] *[…]. Exactement comme moi, avec mes fournisseurs, je vais demander les certificats »*. (Ent.9, numérique et santé). L'entreprise face aux exigences de conformité et de sécurité très fortes demandées par ses clients a de plus instauré depuis deux ans des *« certifications de contrôle »* établies par des tests réalisés par des cabinets d'audits connus qui viennent auditer leur système d'information. Ainsi, les entreprises enquêtées s'alignent sur les attentes de leurs clients, voire revendiquent la satisfaction de leurs clients : *« ce que pensent nos clients c'est important […] la sensibilité qu'ils ont sur leurs données, le fait qu'elles soient correctement traitées »* (Ent.8, transport et logistique).

L'effet ricochet : évaluer la maturité de ses fournisseurs… faire monter le niveau

La cybersécurité devient, pour certains secteurs, un critère dans le choix des partenaires commerciaux (*B to B*). Les entreprises qui ne peuvent pas démontrer leur conformité aux normes de sécurité et réglementations peuvent se retrouver écartées des possibilités de marchés : *« tout le monde doit avoir un certain niveau maintenant »*, où en matière d'hébergement par exemple, la norme ISO 27001 est quasi systématiquement requise pour pouvoir répondre à un appel d'offres, souligne un enquêté (Ent.2). Autre exemple, dans le secteur de la santé, la certification HDS (Hébergement de Données de Santé) est devenue indispensable pour participer à des projets. Ces exigences réglementaires deviennent donc de surcroît un critère de sélection des partenaires et les entreprises qui ne respectent pas ces normes ou les exigences attendues par le secteur d'activité risquent au fil du temps de perdre des contrats ou de diminuer leurs chances d'en obtenir.

[30] *Digital Operational Resilience Act* (DORA), règlement européen sur la résilience opérationnelle numérique du secteur financier.

> « Ce n'est pas une garantie parce que quelque part, ça ne nous garantit pas que […] nous donnera toujours des contrats, c'est clair… Maintenant, celui qui ne s'y colle pas, ils vont peut-être moins le choisir dans leur *supply chain*, ça c'est… mais ils ne vont pas le dire… enfin je ne pense pas. » (Ent.7, industrie).

> « Il y a certains clients qui commencent à se dire que ça va être un prérequis pour travailler avec eux. Donc, d'ici un ou deux ans, ça va aller assez vite, il y en a certains qui vont l'imposer et si on n'est pas [labellisé par ce programme[31]] on ne pourra pas être dans le panel de fournisseurs. » (Ent.5, industrie).

La mise en place de mesures de protection cyber et l'évaluation continue de l'efficacité de ces mesures, leur ajustement permanent, apparaît tout autant stratégique pour la pérennité de l'entreprise sur le plan de la sécurité, que sur le plan commercial. En ce sens, elle peut impacter les possibilités de développement d'une entreprise. Répondre aux exigences de ses clients ou grands donneurs d'ordre par exemple, peut donc aussi être une manière pour les clients de *« fiabiliser leurs sourcings »* en s'assurant de la part de leurs fournisseurs d'un niveau de maturité cyber certain, éprouvé (testé) voire prouvé par des certifications ou un programme progressif de mise en conformité technique et réglementaire qui joue un rôle de « labellisation ».

> « Vis-à-vis des clients, de plus en plus, on est challengé. Donc on a besoin de remplir des questionnaires pour les appels d'offres. Donc ça c'est quelque chose de compliqué parce que ça prend beaucoup de temps. Donc on essaye aussi de travailler pour structurer notre message. Donc typiquement on travaille depuis quelques mois sur la mise en place de PASS enfin des plans d'assurance sécurité, dans les deux sens, pour évaluer la maturité de nos fournisseurs parce que c'était quelque chose qui n'était pas fait au préalable ». (Ent.10, logistique)

Pour les entreprises enquêtées qui ont pleinement intégré la cybersécurité dans leur politique de gouvernance, elle devient aussi un argument concurrentiel, direct ou implicite. En investissant dans des solutions de sécurité avancées, en développant les certifications nécessaires aux exigences de conformité de leurs clients, elles peuvent rassurer leurs clients sur la fiabilité de leurs services. Dans cette démarche proactive engagée, la conformité réglementaire devient de plus en plus contraignante. Les entreprises doivent non seulement se conformer aux exigences, démontrer leur engagement envers la cybersécurité pour se démarquer sur le marché, et certaines, parmi les plus engagées et avancées dans le processus, font réaliser des audits externes réguliers et cherchent à s'assurer, par ricochet, que leurs fournisseurs respectent également des normes de sécurité élevées : *« Donc c'est aussi faire monter le niveau de maturité de tous les acteurs »* (Ent.10).

> « Moi, ce que je demande, c'est que tous les fournisseurs soient évalués pour, entre guillemets, avoir le tampon. Et à l'inverse, ce qu'on travaille aussi, c'est de montrer globalement notre posture sécurisée basée. Enfin on n'est pas certifié ISO, mais on s'en inspire de ces normes-là pour justement avoir un cadre et dire à nos clients, voilà on travaille, on a une gouvernance, on a des plans de sauvegarde, on a des plans de reprise d'activité. […]. Je pense que c'est quelque chose qui devient un peu impactant sur notre métier actuellement. C'est toutes ces preuves à fournir à l'extérieur. » (Ent.10, logistique)

Le partage des actions menées et les preuves d'un niveau de maturité en matière de cybersécurité avec leurs clients, peuvent renforcer la confiance et ainsi améliorer les relations commerciales en construisant des *« partenariats de confiance »*.

> « Quand je suis avec mes patrons, c'est… Et les fois où j'étais avec eux en clientèle ou en réunion interprofessionnelle, c'est clairement une chose qu'on met en avant, en disant, voilà, on est parti de rien, on a mis en place ça parce qu'on a été pris dans le cadre de France Relance et ainsi de suite. C'est clairement assumé de la direction de dire on a été accompagné là-dessus, ça nous a permis d'avoir une maturité supérieure sur ces domaines-là… Le 4.0, la digitalisation, la cyber et ainsi de suite donc c'est pas on ne se cache pas derrière. » (Ent.7).

Paradoxalement, dans un environnement de plus en plus exigeant, la cybersécurité n'apparaît plus seulement considérée comme une contrainte pour ces entreprises, mais comme un levier stratégique pour l'innovation et la compétitivité. En ce sens, au-delà de la protection contre les cyberattaques, la résilience des entreprises devient une valeur, qui concourt au développement d'une « chaîne des exigences » ou de garanties attendues entre clients et fournisseurs. Et le législateur qui visait jusqu'à présent en priorité les opérateurs d'importance vitale et les entités critiques, essentielles ou importantes s'intéresse également à l'intégralité de la chaîne comme en témoigne le règlement sur la cyber-résilience (le *Cyberresilience Act* ou CRA adopté le 10 octobre 2024). Pour

[31] Nom du programme remplacé.

les fournisseurs, non seulement cela se transforme de plus en plus en enjeu concurrentiel, mais cela va également devenir une obligation légale qui s'applique à eux directement.

En résumé : la gestion de la cybersécurité dans les entreprises enquêtées se structure progressivement (créations de poste au sein de l'entreprise voire en inter-entreprises, intégration à la stratégie numérique et à la gouvernance). Toutefois, elle semble souffrir du manque de ressources humaines pour atteindre sa pleine normalisation. De plus en plus exigeantes sur la question cyber, les relations commerciales entre les entreprises représentent un levier pour la mise en conformité. La stratégie cybersécurité devient un argument concurrentiel ; la résilience des entreprises se transforme en valeur.

Conclusion – Des constats aux leviers d'action

Réalités et tensions observées

Les entreprises bretonnes enquêtées ont une conception et une gestion pragmatique de la cybersécurité : *« Il faut rester raisonnable par rapport à la taille de structure qu'on est. »* (Ent.7). L'existence d'une sécurisation cyber est à *minima* technologique et technique et externalisée par une délégation de la gestion de la protection des systèmes d'information et des données à un ou des prestataires, par exemple pour une des plus petites PME enquêtée. Pour d'autres, notamment plus importantes en taille, on observe un mouvement réel enclenché pouvant aller jusqu'à l'intégration d'une politique stratégique de la cybersécurité dans la gouvernance avec l'entrée dans un programme progressif constitué de différents niveaux et une évolution continue de la sécurisation du système d'information de gestion (*IT*), puis une étendue déjà projetée, voire anticipée dans les budgets pour certaines, vers le développement, aussi nécessaire, de la sécurisation de l'informatique de système industriel (*OTI*) *: « on a forcément changé toute notre organisation, la vision et ça a aussi changé le budget »*, souligne un enquêté d'une PME du secteur industriel (Ent.5).

Associée à ces déploiements technologiques et techniques opérés dans un premier moment de la cyber sécurisation, une dimension réglementaire forte et organisationnelle qui comprend la description de procédures à suivre en cas d'incidents (plans de gestion de crise, plan de continuité de l'activité, plan de reprise de l'activité en cas d'incident majeur) est soit très récente ou en train de se mettre en place, soit envisagée dans un second temps. En parallèle, de manière concomitante et interactive, le champ de l'information professionnelle est un axe essentiel du métier de l'informatique, non seulement, parce que le contexte des menaces cyber et les technologies évoluent en permanence, pour mettre en place les systèmes requis et correspondants au plus près des besoins et du fonctionnement de l'activité de l'entreprise, mais aussi pour pouvoir mener au mieux un travail de sensibilisation et de formation des collaborateurs jugé primordial par tous les interlocuteurs : parce que dans les attaques, *« souvent la problématique c'est l'humain »* (Ent.2).

Le plus complexe dans ce processus est vraisemblablement de *« rattraper une dette technique »* due à un sous-investissement longtemps chronique pour des entreprises d'envergure notamment internationale, qui se sont construites originairement sans *IT* et dont l'*IT* ne constitue donc pas le cœur de l'activité : *« Le but, ce n'est pas de faire le mieux de l'état de l'art, de tout ce qui est IT. Le mieux, c'est de transporter des passagers. C'est ça, notre activité. Et l'IT, c'est une fonction support »*, précise un enquêté (Ent.8, transport et logistique). L'activité de l'entreprise, sa vision d'elle-même, et les besoins accrus qu'impose en investissements tant techniques qu'humains (postes et démultiplication de nombre de prestataires, temps des équipes) la protection des systèmes d'information, influent donc considérablement sur la conception de la cybersécurité et le poids qu'elle prend ou non dans la stratégie des entreprises.

Pour autant, les entreprises enquêtées prennent la mesure des enjeux qui se jouent dans la mise en conformité technologique et réglementaire, parce que les orientations défendues et programmées font sens pour les acteurs enquêtés : *« sur la base, c'est beaucoup de bon sens, c'est beaucoup de structuration de données, de structuration d'informations »* (Ent.7, industrie). Les enquêtés sont aussi unanimes sur les coûts exorbitants non seulement de la mise en conformité par des instruments technologiques nombreux, variés et évolutifs, mais aussi des instruments de contrôle (certifications, audits interne et externe, tests de vulnérabilité, tests d'intrusion, etc.) et

de la mesure continue de l'efficacité des systèmes d'information déployés, avec les plans de remédiation et les nouveaux investissements qu'ils imposent. Les freins sont principalement budgétaires, pour *« quelque chose »* qui peut être considéré comme *« ne dégageant pas de valeur »,* perçu comme sans retour sur investissement pour la productivité globale, et générer une certaine gêne à la présentation de budgets d'investissements *« colossaux »* (Ent.3). Seul un entretien évoque la connaissance des programmes d'aides existants et les aides effectivement obtenues dans le cadre d'accompagnement de clusters industriels (ex. les programmes BreizhFab pour les industriels bretons et France Relance du GIFAS[32] pour le secteur de l'aéronautique) ; ce qui laisse supposer un manque d'informations et une faible identification des supports financiers existants tant au niveau national que régional.

Pour d'autres entreprises, particulièrement celles du secteur du numérique, la cybersécurité est centrale, au fondement de l'activité pour laquelle la certification ISO 27001 devient incontournable, « *une évolution naturelle »* du métier tant pour le développement du code (*Secure by design*) que pour l'hébergement des données des clients, pour *« mettre en place des bonnes pratiques, des bons processus »* dès le départ pour *« protéger au mieux ».* Et ce malgré un certain fatalisme qui émane des discours face à un processus continuellement *« en train de se faire »*, qui ne sera *« jamais parfait »*, *« on ne fait que ralentir l'attaquant »*, *« ils ont toujours de l'avance par rapport à ce qu'on fait »* (Ent.2, numérique et hébergement).

Enfin, si la cybersécurité est une « contrainte normative » (technique, normes et réglementation) dans un environnement de plus en plus exigeant, elle porte, en tant que telle, l'essence même de la vocation des normes en incitant à la preuve de garanties, de plus en plus attendues de la part des clients et de plus en plus demandées aux fournisseurs, créant de la sorte par répercussion, à travers le partage des bonnes pratiques et des actions réalisées un levier stratégique en chaîne recherché. Ce que les entreprises enquêtées qui ont intégré la cybersécurité dans leur politique de gouvernance ont bien compris.

Problématiques transversales et dimensions de maturité

Au-delà de la diversité des situations décrites, plusieurs problématiques communes traversent les témoignages recueillis. Ces lignes de tension, présentes dans la majorité des entreprises interrogées, révèlent des freins systémiques et l'appropriation de la cybersécurité en entreprise.

La dépendance aux prestataires externes :

Plusieurs entreprises, notamment les PME industrielles ou des structures de taille intermédiaire, ont exprimé une forte dépendance à leur prestataire informatique externe pour tout ce qui relève de la cybersécurité. Cette dépendance vis-à-vis des prestataires externes traduit, à la fois une contrainte économique structurelle (externalisation par défaut), un manque de structuration interne, en particulier l'absence de référent cybersécurité identifié, et parfois une vision technique de la cybersécurité, réduite à des interventions ponctuelles sans pilotage stratégique. Elle fragilise la réactivité en cas d'incidents, limite l'appropriation des enjeux en interne et rend plus difficile le développement d'une stratégie de résilience à long terme.

Gouvernance cybersécurité faible ou absente :

Dans plusieurs entreprises interrogées, la cybersécurité souffre d'un manque de structuration organisationnelle claire. Ce déficit de gouvernance se manifeste par l'absence de RSSI ou de référent cyber en interne, une cybersécurité poussée par la DSI groupe sans pilotage stratégique local, l'absence de comité cybersécurité, de tableaux de bord ou de reporting régulier à la direction ainsi qu'une marge de manœuvre faible pour décider d'orientations ou de priorités en matière de sécurité numérique. Ce type de situation est fréquent dans les structures industrielles de taille intermédiaire, souvent en transition numérique, où l'IT est présent mais la cybersécurité n'est pas encore pensée comme une fonction autonome. Ainsi, sans pilotage interne, les entreprises restent souvent dans une logique réactive, dépendantes des exigences extérieures (clients, prestataires ou réglementation), et peinent à inscrire la cybersécurité dans leur gouvernance globale.

[32] Groupement des Industries Françaises Aéronautiques.

Pression sectorielle et réglementaire croissante :

Certaines entreprises évoluent dans des secteurs fortement régulés ou soumis à une vigilance accrue de leurs clients (mutuelles, défense, aéronautique, transport, hébergement de données, santé). Dans ce contexte, la cybersécurité n'est pas simplement une bonne pratique, mais un prérequis commercial ou contractuel. Elle devient un facteur d'éligibilité aux appels d'offres, un critère de renouvellement de contrats, voire un élément d'audit imposé par les partenaires. Cette situation crée une pression externe forte : elle pousse certaines entreprises à accélérer leur transformation cyber, parfois à marche forcée, sans toujours disposer de ressources internes pour suivre le rythme. Cette problématique met en évidence un phénomène majeur : la cybersécurité devient une exigence économique, et non plus seulement technique. Les entreprises concernées ne peuvent ni différer, ni minimiser leurs efforts de sécurisation, sous peine de perdre leur légitimité commerciale. Cela crée un levier fort pour encadrer une stratégie cybersécurité, mais aussi un risque de pilotage par l'urgence ou par la contrainte, sans vision long terme. Certaines entreprises choisissent de transformer cette contrainte en levier stratégique, notamment en valorisant leur maturité cyber dans leur relation client. D'autres, en transition, cherchent encore à se mettre à niveau pour rester dans la course.

Manque de sensibilisation et de culture cyber en interne :

La cybersécurité ne se limite pas aux outils ou aux obligations réglementaires : elle dépend aussi, de façon critique, du comportement des collaborateurs. Or, plusieurs entreprises interrogées soulignent un manque de sensibilisation, voire une absence de culture cybersécurité au sein de leurs équipes. Ce manque de culture cyber reflète souvent une absence d'intégration du numérique dans les usages quotidiens, une sous-estimation des risques liés aux comportements humains, et parfois un décalage entre les outils mis en place et les pratiques effectives des utilisateurs. Il représente une faille majeure dans la chaîne de sécurité : les meilleures technologies ne suffisent pas si les collaborateurs ne sont pas formés ni impliqués. Dans certaines entreprises, la sensibilisation commence à être mise en œuvre, mais elle reste encore ponctuelle, non systématisée, ou mal adaptée au terrain.

Préparation insuffisante à la gestion d'incident et à la résilience :

Plusieurs entreprises reconnaissent une faible capacité à gérer un incident cyber de manière structurée. Cette faiblesse se traduit par l'absence ou l'inachèvement de dispositifs tels que : le plan de continuité de l'activité, le plan de reprise d'activité, les procédures de gestion de crise, ou encore des exercices de simulation pour tester la réactivité. Face à une attaque, certaines entreprises envisagent encore une réaction improvisée, reposant sur le prestataire externe, sans plan formalisé ni rôle défini en interne. L'absence de planification en cas d'incident trahit une vision encore défensive de la cybersécurité, où la priorité est donnée à la prévention, mais sans anticipation suffisante de scénario de crise. Les causes principales identifiées sont les suivantes : un manque de temps et de ressources pour formaliser les procédures, une sur-confiance dans la technologie ou dans les prestataires, et une difficulté à se projeter dans une logique de crise, surtout dans les structures de taille modeste. Ce déficit de résilience organisationnelle constitue un point faible critique : en cas de cyberattaque, il peut entraîner des conséquences financières, opérationnelles et réputationnelles majeures, faute d'un dispositif de réponse clair.

Enjeux émergents liés à l'intelligence artificielle :

L'essor rapide de l'intelligence artificielle, en particulier des IA génératives, soulève de nouvelles préoccupations cybersécurité pour plusieurs entreprises interrogées. Même si elle ne constitue pas encore un axe stratégique structurée dans la plupart des cas, l'IA est perçue comme un facteur émergent d'incertitude, de risque et de transformation. Les préoccupations exprimées concernent principalement le risque accru de sophistication des attaques. L'apparition de l'IA dans les discours traduit une prise de conscience diffuse grandissante : les outils d'IA représentent à la fois une menace amplificatrice des risques cyber et un terrain flou d'expérimentation en entreprise.

Ces problématiques ne constituent pas des failles ponctuelles, mais bien des axes de transformation potentiels. Elles invitent à repenser la cybersécurité non pas comme un empilement d'outils ou une simple conformité réglementaire, mais comme un projet collectif, structurant, évolutif et transversal. Leur analyse permet de faire émerger des écarts significatifs entre les entreprises interrogées, aussi bien dans leur manière de percevoir le risque cyber que dans la structuration de leur réponse. Ces écarts ne tiennent pas seulement compte de la taille

de l'entreprise, de son secteur ou de ses moyens techniques. Ils renvoient à des logiques internes différenciées, à des représentations contrastées de la cybersécurité, à des degrés d'appropriation plus ou moins profonds. C'est à partir de cette observation que s'est imposée la nécessité d'introduire une grille de lecture centrée sur **la maturité cybersécurité**.

Les personnes interrogées ne parlent pas toujours directement de « maturité », mais leurs propos révèlent des éléments clés qui permettent de reconstruire ce que signifie pour elles être plus ou moins avancé en cybersécurité. Les dimensions de la maturité, telles qu'elles émergent des discours, renvoient à plusieurs éléments. En premier lieu, l'autonomie dans les choix stratégiques. Être mature, ce n'est pas subir, c'est avoir une stratégie cyber propre, cohérente avec l'activité. En second lieu, la capacité à structurer et à gouverner : la maturité se manifeste par une gouvernance identifiée, c'est-à-dire un responsable, un pilotage, un relais interne. Ainsi lorsqu'une entreprise déclare que *« c'est la DSI du groupe qui décide, localement on applique »*, cela indique une maturité partielle ou déléguée. La troisième dimension de la maturité, c'est l'intégration dans le quotidien : plus qu'un plan ou une politique, la maturité s'observe dans les pratiques quotidiennes (prise de conscience des risques par des équipes, campagnes de phishing tous les trimestres). La quatrième dimension est la résilience et la capacité à faire face : une entreprise mature ne se limite pas à prévenir, elle se prépare aussi à réagir (test de son PRA deux par an, par exemple). La cinquième dimension, enfin, c'est l'anticipation des transformations : la maturité s'exprime ici dans la capacité à intégrer des enjeux émergents (attaques via l'IA).

Ainsi, ***la maturité cybersécurité, telle qu'elle émerge des entretiens peut se définir comme la capacité d'une entreprise à piloter de manière plus ou moins autonome, cohérente et anticipatrice sa sécurité numérique, en l'intégrant dans ses pratiques, sa gouvernance et ses choix stratégiques, plutôt qu'en la subissant***. Cette maturité est à la fois technique, organisationnelle, culturelle et stratégique. Elle se manifeste dans la manière dont l'entreprise structure sa gouvernance, l'appropriation collective du sujet par les collaborateurs, la capacité à prévenir, réagir et à évoluer face aux menaces et à la place qu'occupe la cybersécurité dans les arbitrages stratégiques.

Typologie des profils et leviers d'accompagnement différenciés

Sur la base des dimensions ci-avant citées, les entreprises interrogées peuvent être regroupées en trois profils types, correspondant à des stades d'avancement distincts dans la structuration de leur cybersécurité. Cette typologie ne vise pas à juger : elle propose une grille de lecture pragmatique, permettant d'ajuster des interventions d'accompagnement selon les réalités de chaque entreprise.

Profil 1 : les entreprises à maturité cybersécurité avancée

Ces entreprises ont intégré la cybersécurité comme une composante stratégique de leur fonctionnement. Elles ne se contentent pas de répondre à des obligations réglementaires : elles développent une vision proactive, structurée et transversale, dans laquelle la sécurité numérique est perçue comme un levier de continuité, de confiance et d'excellence opérationnelle. Certaines vont plus loin encore, en intégrant les enjeux émergents tels que l'intelligence artificielle, la gestion du risque fournisseur, ou la désinformation. Dans ces entreprises, la cybersécurité est élevée au rang de préoccupation stratégique, souvent en lien avec des enjeux critiques : protection des données clients, services vitaux, dépendance à la *supply chain*. La direction générale est engagée, les métiers sont impliqués, et la DSI ou la sécurité n'est plus seule en responsabilité. Ces entreprises font preuve d'anticipation, d'autonomie et de culture réflexive, ce qui les rend capables de s'adapter à l'évolution rapide des menaces : elles illustrent une approche mature et systémique de la cybersécurité.

Profil 2 : Les entreprises à maturité intermédiaire ou en transition

Ce deuxième groupe rassemble des entreprises qui manifestent une prise de conscience nette et forte, mais dont la cybersécurité reste en construction, incomplète ou partiellement dépendante d'acteurs externes. Ces entreprises ne sont pas en retrait, mais en phase de structuration, souvent stimulées par des contraintes externes (exigences clients, audits fournisseurs, pression sectorielles). Ces entreprises sont à un carrefour organisationnel : elles savent qu'elles doivent progresser, mais ne disposent pas toujours des ressources, des compétences internes ou de temps pour formaliser une démarche complète. Elles avancent souvent par

réaction, sans toujours maîtriser le calendrier ni le périmètre. Ce profil traduit une ambivalence typique des entreprises en évolution numérique : entre volonté de faire mieux et contraintes du quotidien. Leur enjeu central est de consolider leur gouvernance interne et de développer une appropriation collective du risque cyber. Ces entreprises incarnent une maturité intermédiaire, évolutive, guidée par l'environnement plutôt que par une stratégie initialement volontaire.

Profil 3 : Les entreprises à maturité cybersécurité faible ou fragmentaire

Dans ces entreprises, la cybersécurité reste une fonction périphérique, technique et largement externalisée. Elle est souvent perçue comme un poste de dépense non prioritaire, voire comme un enjeu abstrait par les équipes non techniques. La dépendance aux prestataires est forte, les responsabilités sont floues, et l'appropriation interne du sujet est limitée. Ce profil d'entreprises est le plus vulnérable face aux menaces actuelles. Il reflète souvent une combinaison de manque de moyens, de culture technique et de légitimation stratégique du sujet. Cependant, ces entreprises ne sont pas dans le déni : certaines expriment de l'inquiétude face à ce qu'elles savent être un « point faible ». Ce groupe ne manifeste pas de rejet de la cybersécurité, mais plutôt un manque d'appropriation et de projection. Le sujet reste périphérique, sans ancrage stratégique clair. Ces entreprises ont besoin d'un accompagnement ciblé, progressif et pédagogique, visant à construire les fondations organisationnelles d'une démarche cyber : référent interne, culture minimale, évaluation des risques métier.

Cette typologie permet de mettre en évidence des logiques différenciées d'appropriation de la cybersécurité par les entreprises bretonnes. Le premier groupe se caractérise par une approche proactive et structurée. Dans le second groupe, on retrouve une approche réactive mais évolutive. Dans le troisième groupe, enfin, la cybersécurité semble contrainte, minimale ou symbolique. Cette typologie ne vise pas à hiérarchiser les entreprises : elle a pour but de comprendre les conditions concrètes de leur engagement en cybersécurité. Certaines progressent parce qu'elles ont anticipé. D'autres parce qu'elles sont contraintes. D'autres encore n'en perçoivent pas encore la pleine portée.

En rendant visibles les profils et leurs besoins respectifs, cette typologie devient un outil pour la décision publique et l'action collective. Elle peut guider : la conception de parcours d'accompagnement différenciés (formations, cofinancements, audits), le ciblage des aides à l'investissement cyber, la priorisation des actions collectives (par secteur, taille, niveau de risque), le positionnement de la cybersécurité comme levier transversal dans les politiques numériques, industrielles ou des ressources humaines.

Références

Arpagian Nicolas, 2022, Cybersécurité, PUF, Que sais-je, (4e édition).

Auray Nicolas, Kaminsky Danielle, 2008, Les trajectoires de professionnalisation des hackers : la double vie des professionnels de la sécurité, *Annales des Télécommunications*, 62, n°11-12, pp.1313-1327.

Annexes

Annexe 1 : le cadre légal cité

1. **Le *Cybersecurity Act* (UE 2019/ 881)**, publié le 7 juin 2019, définit le cadre européen de certification de cybersécurité. Il entrera en application à partir du 11 décembre 2027 (article 71, du Règlement sur la cyber-résilience). Il s'agit d'un schéma directeur qui établit plusieurs niveaux d'assurance avec sa méthodologie d'évaluation associée (niveaux élémentaire, substantiel, élevé). Cette réglementation s'adresse aux fabricants et fournisseurs de produits, services et processus technologiques de l'information et communication (TIC) pour qui elle fixe un ensemble d'exigences de sécurité. Elle concerne aussi les organismes d'évaluation de la conformité pour délivrer des certificats de cybersécurité européens avec les méthodes d'évaluation robustes et harmonisées. Elle concerne les utilisateurs finaux et donneurs d'ordre afin de leur permettre d'utiliser et choisir les produits TIC, services TIC et processus TIC correspondant à leur besoin de sécurité. Cf. https://cyber.gouv.fr/cybersecurity-act

2. La **Directive européenne NIS** (27 décembre 2022) impose aux Etats membres de l'Union européenne d'adopter des stratégies nationales de cybersécurité et de désigner des autorités compétentes pour superviser la sécurité des réseaux et des systèmes d'information. Cela inclut la création de réseaux de centres de réponse aux incidents (CSIRT) pour assurer une coopération efficace et le partage d'informations. Puis la Directive européenne NIS2 entre en vigueur le 17 octobre 2024. https://cyber.gouv.fr/la-directive-nis-2 .

3. 23 janvier 2023 : adoption de la **loi d'orientation et de programmation du ministère de l'intérieur** (LOPMI) destinée en partie à répondre aux nouveaux enjeux de lutte contre la cybercriminalité – et la loi d'orientation et de programmation du ministère de la justice (LOPMJ, 20 novembre 2023). L'apparition de nouvelles infractions dans le droit français : l'enjeu principal de la LOPMI est la lutte contre les écosystèmes criminels présents sur Internet ; la loi a créé d'une part le délit d'administration d'une plateforme en ligne proposant des produits illicites, d'autre part le délit d'intermédiation ou de séquestre pour les plateformes en facilitant la revente. Le 17 février 2024 : entrée en vigueur du ***Digital Service Act* (DSA)** applicable dès le 23 août 2023 pour « les très grands moteurs de recherche ».

4. Sous le contrôle de l'ARCEP, l'ANSSI dispose notamment de dispositifs légaux de détection et d'anticipation, en particulier **la Loi de Programmation Militaire 2024-2030** modifiant le code des postes et des communications électronique (CPCE) et le code de la défense.

5. **Le règlement DORA** entré en vigueur le 17 janvier 2025 renforce la résilience opérationnelle numérique des entités financières face aux cybermenaces et aux risques liés aux Technologie de l'Information et de la Communication.

6. **La norme ISO/CEI 27032** joue un rôle crucial en fournissant un cadre pour la cybersécurité en aidant les entreprises à identifier leurs vulnérabilités et à mettre en place des pratiques de protection efficaces.