UCLouvain

LOUVAIN
School of Management

Louvain School of Management

Vers une intégration de la Cybersécurité comme un élément de matérialité dans la CSRD

Quand la protection des systèmes rime avec responsabilité sociétale

Auteur : Adrien DEFER
Promoteur : Corentin HERICHER
Année académique 2025-2026
Travail de fin d'études (TFE) en vue d'obtenir le titre de
Master [60] en Sciences de Gestion
Horaire décalé

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Louvain School of Management

Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique

www.uclouvain.be/lsm

Résumé

La cybersécurité est aujourd'hui un enjeu majeur pour l'ensemble des secteurs d'activité. Les cyberattaques se multiplient et touchent indistinctement les secteurs financier, industriel, public, mais aussi ceux de la santé, de l'énergie, des télécommunications, du commerce, des transports ou encore de la technologie. Aucune organisation n'est à l'abri, quels que soient sa taille ou son domaine.

Malgré l'importance croissante de ces menaces, il existe encore peu de dispositifs de reporting public harmonisé sur la cybersécurité. Certaines réglementations européennes, comme le RGPD ou la directive NIS2, imposent la communication d'informations après certains incidents, mais cela reste occasionnel. Le règlement DORA, quant à lui, introduit des obligations de résilience opérationnelle et de reporting plus strictes, mais limitées au secteur financier.

Ce mémoire propose d'étudier la possibilité d'intégrer plus systématiquement la cybersécurité dans le reporting de durabilité prévu par la directive européenne CSRD (Corporate Sustainability Reporting Directive). Si certains aspects liés à la cybersécurité sont déjà évoqués dans des normes comme ESRS 2 ou ESRS G1, cela n'est fait que lorsque l'entreprise juge le sujet « matériel » au sens de la double matérialité.

L'objectif du mémoire est donc d'examiner dans quelle mesure la cybersécurité pourrait être considérée comme un élément de matérialité à part entière, au même titre que les enjeux financiers ou d'impact. Cela permettrait aux parties prenantes d'évaluer non seulement la durabilité d'une entreprise, mais aussi sa capacité à se protéger contre les risques numériques qui menacent sa résilience.

Cette réflexion se limite à l'analyse des directives européennes existantes, sans entrer dans les détails des transpositions nationales ni des exigences locales propres à chaque État membre.

Avant-Propos

Je tiens à remercier mon promoteur, Corentin HERICHER, pour son accompagnement bienveillant et ses conseils avisés tout au long de ce mémoire. Je remercie également Thomas DEMONTY pour son soutien constant et ses retours constructifs. Enfin, ma reconnaissance s'adresse à tous mes proches qui m'ont encouragé durant cette période de recherche.

Table des Matières

1 Introduction

Depuis plusieurs années, les entreprises européennes sont confrontées à une transformation profonde de leurs obligations en matière de transparence extra-financière. La **Corporate Sustainability Reporting Directive (CSRD)**, entrée en vigueur le **5 janvier 2023**, marque une étape décisive dans cette évolution. Elle remplace progressivement la **Non-Financial Reporting Directive (NFRD)**, avec un champ d'application élargi à plus de **50 000 entreprises** dans l'Union européenne [30], contre environ **11 700 auparavant** [23]. En imposant la publication d'informations précises, vérifiables et standardisées [19] sur les enjeux environnementaux, sociaux et de gouvernance (ESG), la CSRD s'inscrit dans une volonté politique forte de réorienter les flux de capitaux vers une économie plus durable.

L'une des caractéristiques structurantes de la CSRD est l'adoption du principe de *double matérialité* : les entreprises doivent désormais rendre compte non seulement de l'impact financier des enjeux ESG sur leurs activités, mais aussi de l'impact de leurs activités sur la société et l'environnement, les ressources naturelles, le climat, et la société en général [44]. Cette approche renforce considérablement la responsabilité des entreprises en matière de durabilité et les incite à identifier de manière exhaustive les risques, opportunités et impacts associés à leur modèle économique. Pour les guider, l'**European Financial Reporting Advisory Group (EFRAG)** a élaboré les **European Sustainability Reporting Standards (ESRS)**, qui précisent les attentes en termes de contenu, de format et de méthodologie des rapports.

Toutefois, dans cette dynamique de transformation, un domaine critique demeure encore insuffisamment représenté dans les pratiques de reporting : la *cybersécurité*. Alors même que les cyberattaques augmentent en fréquence et en gravité, affectant tant les grandes entreprises que les PME, la cybersécurité est rarement considérée comme un facteur de matérialité ESG à part entière. La norme ESRS 2 (General Disclosures) évoque la sécurité de l'information de manière marginale, principalement à travers **IRO-1** (processus d'évaluation de la matérialité), **GOV-5** (gestion des risques et contrôles internes) et **SBM-3** (prise en compte des risques matériels dans la stratégie), sans faire l'objet d'un traitement spécifique ou approfondi [24]. Cependant, aucune norme sectorielle spécifique ne prévoit, à ce jour, une exigence robuste de reporting sur la gestion

des risques cyber. Cela contraste avec la réalité du terrain, où la cybersécurité est devenue un enjeu transversal, affectant la *gouvernance*, la *résilience opérationnelle*, la *confidentialité des données*, la *réputation*, voire les *performances financières* d'une entreprise.

Il existe cependant plusieurs référentiels et réglementations encadrant la gestion et la diffusion d'informations liées à la cybersécurité, tels que le **NIST Cybersecurity Framework version 2**, le **General Data Protection Regulation (GDPR)** et le **Digital Operational Resilience Act (DORA)**. Toutefois, seuls DORA, qui s'applique exclusivement au secteur financier, et le RGPD imposent des obligations spécifiques de communication : DORA exige la déclaration des incidents cyber majeurs aux autorités de supervision [20], tandis que le RGPD impose la notification des violations de données personnelles aux autorités compétentes et, dans certains cas, aux personnes concernées [18]. En dehors de DORA, la publication de données liées à la cybersécurité n'est donc pas systématique et dépend généralement de la survenue d'événements externes, tels qu'une attaque ou une violation de données. En revanche, NIST 2 est un cadre volontaire [1] qui ne prévoit aucune obligation de publication ou de communication publique des données cyber [40].

Ce décalage entre la matérialité effective des risques cyber et leur traitement réglementaire soulève une série de questions fondamentales. La cybersécurité ne devrait-elle pas être intégrée de manière systématique dans les *matrices de double matérialité* ? Quels indicateurs ou méthodologies permettraient de mieux capter la réalité de cet enjeu dans les rapports de durabilité ? Et comment faire en sorte que les fonctions de cybersécurité, souvent rattachées à la direction informatique, dialoguent de manière structurée avec les responsables ESG et conformité ?

C'est à partir de ce constat que ce mémoire entend explorer la question de recherche suivante, inscrite dans le cadre présenté ci-dessous.

? Question de recherche
Comment intégrer la cybersécurité comme facteur de matérialité dans le cadre de la CSRD ?

L'objectif de ce mémoire est double. D'une part, il vise à démontrer que **la cybersécurité**

1. Bien que le NIST ne soit pas une autorité réglementaire, le Cybersecurity Framework est devenu obligatoire pour les agences fédérales américaines depuis le décret présidentiel 13800. Pour les autres organisations, son adoption reste volontaire, sauf lorsqu'il est exigé par certains clients ou chaînes d'approvisionnement [41].

constitue non seulement un risque financier majeur, mais aussi un sujet à fort impact sociétal et environnemental, susceptible de justifier une place plus centrale dans le reporting de durabilité. D'autre part, il s'agit de montrer que **l'intégration de la cybersécurité comme facteur de matérialité peut contribuer à rediriger les flux de capitaux des investisseurs non seulement vers des entreprises "vertes", mais aussi vers des organisations véritablement résilientes**, capables de faire face aux menaces numériques croissantes. Cette réflexion s'inscrit dans une dynamique plus large de transformation durable de l'économie européenne, que nous aborderons plus en détail à travers l'analyse du *Pacte vert pour l'Europe* et du *Green Deal* dans les sections suivantes.

Pour explorer cette question de recherche à double objectif, ce mémoire s'organisera en plusieurs parties. Après avoir présenté les principaux concepts réglementaires et techniques liés à la CSRD et à la cybersécurité, nous analyserons la manière dont cette dernière est traitée dans les principaux référentiels de durabilité. Une étude de cas centrée sur l'analyse de premiers rapports de conformité à la CSRD permettra ensuite d'évaluer l'état actuel des pratiques. Enfin, des recommandations concrètes seront proposées afin de favoriser une intégration stratégique et opérationnelle de la cybersécurité dans les démarches ESG à venir.

2 Contexte et Concepts Clés

Cette section pose les bases conceptuelles et réglementaires nécessaires à la compréhension du lien entre cybersécurité et reporting de durabilité. Elle revient d'abord sur les fondements de la CSRD, en clarifiant les notions de matérialité et le rôle des acteurs clés comme l'EFRAG. Ensuite, elle définit la cybersécurité et en distingue les enjeux actuels pour les entreprises, avant d'établir les premiers ponts entre la sécurité numérique et la performance durable des organisations.

2.1 Concepts Réglementaires

Cette sous-section regroupe les bases légales et institutionnelles nécessaires à la compréhension du reporting de durabilité tel que redéfini par la CSRD, notamment ses objectifs, le principe de double matérialité, et le rôle des normes européennes élaborées par l'EFRAG.

2.1.1 Définition et Objectifs de la CSRD

Information

Les informations suivantes sont principalement extraites du document de référence officiel, tel que publié dans le Journal officiel de l'UE, qui fait autorité en la matière [19].

La **CSRD (Corporate Sustainability Reporting Directive)** est une directive européenne adoptée en **décembre 2022** qui vise à moderniser et renforcer les obligations de reporting extra-financier des entreprises en matière de durabilité. Elle remplace et élargit l'ancienne directive **NFRD (Non-Financial Reporting Directive)** en imposant à un plus grand nombre d'entreprises européennes - y compris certaines PME - de publier des informations *détaillées*, *fiables*, *comparables* et *vérifiables* sur les impacts environnementaux, sociaux et de gouvernance (**ESG**) de leurs activités.

La CSRD s'inscrit dans le cadre du **Pacte vert pour l'Europe (European Green Deal)** et du **Plan d'action pour la finance durable** de la Commission européenne. Le Green Deal, présenté en **décembre 2019**, constitue la feuille de route stratégique de l'Union européenne pour atteindre la *neutralité climatique* d'ici 2050 [25]. Il vise à transformer profondément l'économie européenne en la rendant *plus respectueuse de l'environnement*, *plus circulaire*, et *plus résiliente face aux risques climatiques*. L'un des piliers du Green Deal est de réorienter les flux de capitaux vers des activités durables, ce qui suppose une transparence accrue sur les pratiques environnementales, sociales et de gouvernance des entreprises. C'est dans cette perspective que s'inscrit le Plan d'action pour financer la croissance durable, adopté en 2018, et qui, comme expliqué dans le document [21], inclut notamment :

- L'établissement d'un langage commun pour la finance durable, autrement dit un **système de classification unifié (taxinomie)** de l'UE.
- La création de **labels de l'UE** pour les produits financiers verts, sur la base de ce système de classification de l'UE.
- La clarifier l'**obligation, pour les gestionnaires d'actifs et les investisseurs institutionnels**, de tenir compte des aspects de durabilité dans le processus d'investissement et renforcer leurs obligations en matière de publication d'informations.

- L'intégration de la **durabilité dans les exigences prudentielles**.
- Le renforcement de la transparence en matière de **publication d'informations par les entreprises**.

La CSRD constitue une réponse concrète à ces objectifs, en imposant aux entreprises de rendre compte de manière **normalisée** et **vérifiable** de leurs impacts ESG, afin de permettre aux investisseurs et aux parties prenantes d'évaluer leur contribution à la *transition durable*. Elle répond à plusieurs constats formulés dans les considérants de la directive 2022/2464 [19].

Considérant n°13

« [...] De nombreux éléments indiquent que de nombreuses entreprises ne publient pas d'informations significatives sur tous les sujets majeurs liés à la durabilité, y compris les informations liées au climat, telles que l'ensemble des émissions de GES et les facteurs qui ont des incidences sur la biodiversité. [...] »

Considérant n°11

« La demande d'informations en matière de durabilité des entreprises a considérablement augmenté ces dernières années, en particulier de la part de la communauté des investisseurs. Cette augmentation de la demande s'explique par l'évolution de la nature des risques pour les entreprises et la sensibilisation croissante des investisseurs aux implications financières de ces risques. [...] »

Pour répondre aux insuffisances constatées dans le cadre précédent et accompagner la transition vers une économie plus durable, la CSRD définit un ensemble d'objectifs structurants. Ces objectifs visent à améliorer la **qualité**, la **portée** et la **vérifiabilité** des informations publiées par les entreprises sur leurs enjeux de durabilité, dans une logique de **transparence**, de **responsabilité** et de **cohérence** à l'échelle européenne. Ils sont précisés dans le corps de la directive ainsi que dans ses considérants, et constituent le socle de la nouvelle stratégie de *reporting extra-financier* de l'Union. Voici, ci-dessous, quelques-uns de ces objectifs, tels qu'énoncés dans le résumé du rapport d'analyse et d'impact de la CSRD [22].

OBJ n°1

> « Garantir que les entreprises dont les informations non financières sont nécessaires aux utilisateurs publient effectivement ces informations, et que celles-ci soient pertinentes, comparables, fiables et faciles d'accès et d'utilisation. »

OBJ n°2

> « [...] Réduire les coûts inutiles pour les préparateurs. En permettant aux investisseurs de mieux évaluer les risques et les incidences des investissements en matière de durabilité, elle mobilisera des financements privés au profit du pacte vert pour l'Europe. »

OBJ n°3

> « [...] Contribuer à l'achèvement de l'union des marchés des capitaux en permettant aux investisseurs d'obtenir des informations non financières comparables de la part des entreprises dans lesquelles ils pourraient investir, et cela, dans toute l'UE. »

OBJ n°4

> « [...] Renforcer le contrat social entre les entreprises et la société, en rendant les entreprises davantage comptables de leur impact sur la société et l'environnement. »

2.1.2 La Notion de Double Matérialité (ou Double Importance Relative)

La directive CSRD repose sur une refonte en profondeur des pratiques de reporting en matière de durabilité, au cœur de laquelle se trouve le principe de double matérialité, ou double importance relative. Ce concept constitue un des fondements théoriques majeurs du nouveau cadre réglementaire et reflète la volonté de l'Union européenne d'intégrer les enjeux environnementaux, sociaux et de gouvernance (ESG) dans une perspective à la fois économique et sociétale. Voici, ci-dessous la définition de ce concept, tel qu'énnoncé dans le considérant n°29 de la directive 2022/2464 [19].

Considérant n°29

« [...] imposent de publier non seulement des informations dans la mesure nécessaire à la compréhension de l'évolution des affaires, des résultats et de la situation de l'entreprise, mais aussi des informations nécessaires à la compréhension de l'incidence des activités de l'entreprise sur les questions environnementales, sociales et de personnel, le respect des droits de l'homme et la lutte contre la corruption. Ces articles obligent donc les entreprises à publier des informations à la fois sur les incidences des activités de l'entreprise sur la population et l'environnement et sur la manière dont les questions de durabilité influent sur l'entreprise.

Il s'agit de la perspective de la "double importance relative", selon laquelle la notion d'importance relative est envisagée de deux points de vue : celui des risques pour l'entreprise et celui des incidences de l'entreprise. [...] »

Introduite initialement dans la directive NFRD (2014/95/UE) [17] et précisée dans la CSRD (2022/2464), la double matérialité repose sur deux dimensions complémentaires : *"La double matérialité combine (i) l'impact de l'entreprise sur l'environnement et la société (inside-out) et (ii) l'incidence financière des enjeux de durabilité sur l'entreprise (outside-in). Les deux perspectives doivent être considérées séparément puis conjointement pour déterminer les divulgations requises ([19], cons. 29)"*. Celles-ci sont particulièrement bien expliquées sur le site du portail du gouvernement français [44]. En voici les définitions, tirées de ce site web.

La matérialité d'impact

« Cette dimension examine les impacts des activités de l'entreprise sur l'environnement, les ressources naturelles, le climat, et la société en général. Il s'agit de déterminer dans quelle mesure les opérations de l'entreprise ont des répercussions positives ou négatives sur ces aspects, au-delà de la simple performance financière. »

La matérialité financière

« La demande d'informations en matière de durabilité des entreprises a considérablement augmenté ces dernières années, en particulier de la part de la communauté des investisseurs.

> Cette augmentation de la demande s'explique par l'évolution de la nature des risques pour les entreprises et la sensibilisation croissante des investisseurs aux implications financières de ces risques. »

Cette approche duale modifie profondément le positionnement stratégique du **reporting de durabilité** [22], en incitant les entreprises à considérer non seulement les **risques** que les enjeux ESG font peser sur leur modèle économique, mais également leur propre **responsabilité** vis-à-vis de l'environnement et des parties prenantes. Elle renforce ainsi la **redevabilité** (*accountability*) des entreprises vis-à-vis de leur écosystème.

La double matérialité est également au centre de la structure des normes ESRS (European Sustainability Reporting Standards) [8], élaborées par l'EFRAG. Ces normes imposent à chaque entreprise une **analyse de matérialité** rigoureuse, structurée selon ces **deux dimensions**, afin de déterminer quelles informations doivent être publiées dans le cadre du reporting de durabilité.

2.1.3 Rôle de l'EFRAG dans l'Elaboration des ESRS

Dans le cadre de la mise en œuvre de la directive CSRD, et comme précisé dans le considérant n°39 de la directive, l'élaboration des normes européennes de reporting de durabilité – les ESRS (European Sustainability Reporting Standards) – a été confiée à un organisme central : l'EFRAG (European Financial Reporting Advisory Group). Historiquement, l'EFRAG a été créé en 2001 à la demande de la Commission européenne, afin de :

- Fournir une expertise technique sur les normes comptables internationales (IFRS).
- Emettre des avis d'homologation à destination de la Commission.
- Représenter la voix de l'Europe dans le développement des normes comptables mondiales.

En 2022, avec l'entrée en vigueur de la CSRD (Corporate Sustainability Reporting Directive), l'EFRAG a vu son mandat s'élargir avec la responsabilité de l'élaboration des normes européennes de reporting de durabilité (ESRS) [14].

La CSRD (directive 2022/2464), notamment à son article 29b, désigne d'ailleurs explicitement l'EFRAG comme conseiller technique de la Commission pour l'élaboration des normes de durabilité. À ce titre, l'EFRAG est chargé de proposer des projets de normes, dans le respect des

exigences de la directive, notamment :

- L'alignement avec le principe de double matérialité.
- La couverture des trois piliers ESG (environnemental, social, gouvernance).
- La cohérence avec les autres normes internationales (ex. : IFRS Sustainability, GRI).
- La prise en compte des besoins spécifiques des parties prenantes (i.e. les investisseurs).

Pour mener à bien cette mission, l'EFRAG s'est doté d'une nouvelle structure dédiée à la durabilité : le **Sustainability Reporting Board** et le **Sustainability Reporting Technical Expert Group**, réunissant experts, représentants d'entreprises, universitaires, régulateurs et membres de la société civile. Ces groupes sont chargés de construire un socle technique **robuste**, **équilibré** et **fondé sur la consultation publique** [14].

En **novembre 2022**, l'EFRAG a soumis à la Commission européenne un premier jeu de normes sectorielles et transversales, regroupées en 12 standards appelés ESRS Set 1 [13]. Ces normes, devenues contraignantes en 2023 pour les grandes entreprises, définissent les exigences en matière de publication d'informations sur les politiques, les objectifs, les plans d'action, les indicateurs et les risques en lien avec les enjeux ESG.

Le rôle de l'EFRAG est donc **essentiel** à la fois sur le plan **méthodologique** – en garantissant la rigueur et la pertinence du cadre de reporting – et sur le plan **opérationnel**, en facilitant l'implémentation concrète de la CSRD par les entreprises concernées. Par cette fonction de normalisation technique, l'EFRAG contribue à assurer la **comparabilité**, la **fiabilité** et la **qualité** des données de durabilité à l'échelle européenne.

2.2 Concepts Techniques

Cette sous-section renvoient aux notions clés liées à la cybersécurité, à ses enjeux actuels pour les entreprises, ainsi qu'à ses liens avec la gouvernance, la résilience opérationnelle et la performance durable.

2.2.1 Définition de la Cybersécurité

Dans le contexte des transformations numériques et des exigences croissantes en matière de durabilité et de gouvernance, il est essentiel de bien distinguer la notion de cybersécurité, qui

constitue un concept à la fois large et stratégique.

Ce concept, relativement récent, est si vaste - avec de nombreux sous-concepts et composants - et utilisé par tant de parties prenantes et de standards en tout genre, que l'on se retrouve dans une situation où il devient impossible d'en dégager une définition unique. Ce phénomène est si réel que l'ENISA (Agence européenne pour la cybersécurité) a publié, en 2015, un document d'une trentaine de pages recensant certaines différences entre les diverses définitions de ce concept. Voici d'ailleurs ci-dessous une définition claire (traduite de l'anglais) issue de l'ITU-T (International Telecommunication Union) [33], citée dans ce document de l'ENISA [16].

Définition de la cybersecurité

« La cybersécurité est l'ensemble des outils, politiques, concepts de sécurité, mesures de sécurité, lignes directrices, approches de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger l'environnement cybernétique ainsi que les actifs de l'organisation et de l'utilisateur.

Les actifs de l'organisation et de l'utilisateur comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunications, ainsi que l'ensemble des informations transmises et/ou stockées dans l'environnement cybernétique.

La cybersécurité vise à garantir l'obtention et le maintien des propriétés de sécurité des actifs de l'organisation et de l'utilisateur face aux risques de sécurité pertinents dans l'environnement cybernétique.

Les objectifs généraux de sécurité comprennent les suivants : la disponibilité, l'intégrité (qui peut inclure l'authenticité et la non-répudiation) et la confidentialité. »

Ainsi, la cybersécurité se situe à l'intersection de la technologie, de la gouvernance, de la stratégie et de la conformité réglementaire. Elle ne se limite pas à la protection des outils, mais englobe également des enjeux humains, juridiques, économiques et de réputation. Dans cette perspective, elle devient un levier de confiance pour les parties prenantes - notamment les clients,

les partenaires, les investisseurs et les autorités - et un critère de performance durable.

2.2.2 Enjeux Actuels de Cybersécurité pour les Entreprises

La cybersécurité est devenue un enjeu stratégique pour toutes les entreprises, quels que soient leur taille ou leur secteur [11]. Avec l'essor du cloud, du télétravail, des objets connectés ou encore de l'intelligence artificielle, la transformation numérique s'accélère - et avec elle, les risques. Les organisations sont désormais confrontées à des menaces de plus en plus nombreuses, qui peuvent avoir des conséquences sérieuses sur leur activité, leur image ou même leur survie.

La cybersécurité soulève de nombreux enjeux, constats et perspectives. Il n'est pas toujours simple de faire ressortir quelques grands axes qui en couvrent l'essentiel. Le document rédigé par l'ESSEC [15] est, à ce titre, une ressource particulièrement intéressante. Il explore en détail les enjeux, les impacts, les leviers d'action, ainsi que d'autres aspects liés à la cybersécurité. Ce rapport met en avant quatre grands enjeux identifiés en 2022, qui me semblent toujours d'actualité aujourd'hui. Ils résument bien, selon moi, les principaux défis auxquels les entreprises doivent faire face dans ce domaine. Certains de ces points seront présentés ci-dessous pour mieux en comprendre la portée.

> ⭐ **Enjeu n°1 - Le marché de la cybersécurité est en pleine croissance**
>
> Le marché de la cybersécurité devrait croître d'environ **12% par an** entre 2022 et 2030, passant de **184,97** à **500,7 milliards de dollars**. Cette croissance est portée par l'augmentation du **coût des cyberattaques**, la généralisation du **télétravail** et le renforcement des **réglementations**. Toutefois, le secteur fait face à des défis majeurs : une **pénurie de personnel qualifié** et le **recours**, notamment dans les **PME**, **à des solutions non licenciées** en raison du coût élevé des outils de cybersécurité.

> ⭐ **Enjeu n°2 - Les conséquences des cyberattaques peuvent être lourdes**
>
> Les conséquences des cyberattaques sont de plus en plus lourdes, notamment sur le plan financier. En France, le coût médian d'une cyberattaque a bondi de ≈ **9.000€** en 2019 à ≈ **46.000€** en 2020, avant de se stabiliser autour de ≈ **20.000€ à** ≈ **19.500€** les

années suivantes. Cette hausse s'explique par la **montée des ransomwares**, le **télétravail** et une **meilleure structuration des attaques**. En parallèle, **58% des entreprises** ont subi au moins une attaque en un an, et certaines ont vu leur **valeur en bourse chuter de 9%**, voire jusqu'à **80% de perte de valorisation pour les ETI** (Entreprises de Taille Intermédiaire). La menace est généralisée : **48% des entreprises dans le monde** ont été touchées récemment, avec **21% des TPE/start-ups** victimes d'au moins une attaque. Même les structures de taille moyenne sont fortement exposées, avec des pertes estimées à **plusieurs millions d'euros** selon leur chiffre d'affaires.

Au-delà des pertes financières, les cyberattaques causent également des **dégâts matériels et opérationnels importants**. Une réaction rapide est essentielle pour limiter leur impact. Celle-ci repose sur trois étapes clés : **la détection des intrusions**, **l'arrêt immédiat de l'attaque**, et **l'évaluation des dommages**. En effet, **17% des entreprises touchées ont subi un vol de données**, tandis que **14% ont connu une destruction de données**. Il est donc crucial de disposer de **plans d'urgence** pour isoler rapidement les réseaux et éviter une propagation à l'ensemble de l'organisation. Notons que 40% des entreprises estiment que leurs propres données sont les plus menacées, contre 30% pour celles de leurs clients.

Enjeu n°3 - La crise du Covid a fragilisé les systèmes d'information des entreprises

La pandémie de Covid-19 a profondément fragilisé les systèmes d'information des entreprises, provoquant une **refonte de leur architecture réseau** et une **généralisation du télétravail** à tous les niveaux hiérarchiques. Cette nouvelle organisation a accru la **vulnérabilité des employés**, souvent contraints d'utiliser des **équipements personnels moins sécurisés**, élargissant ainsi la **surface d'attaque** et compliquant la **surveillance des systèmes**. Les cybercriminels ont su exploiter ce contexte de crise, notamment via des campagnes de phishing utilisant le Covid-19 comme prétexte. Le nombre de cyberattaques a explosé : **+400% en 2020** et **+800% en 2021**, avec une intensification des **attaques DDoS** et des **ransomwares** aux demandes financières élevées. Pourtant, toutes les entreprises n'ont pas pris la mesure de cette menace : **46% des RSSI interrogés ignoraient l'augmentation du risque** avant l'enquête, bien que **70% de ceux qui l'ont constatée**

. **l'attribuent directement à la pandémie**.

Enjeu n°4 - L'infogérance : un enjeu stratégique pour les entreprises

Face à la complexité croissante des menaces, **l'externalisation des services de cybersécurité - ou infogérance-** s'impose comme un **levier stratégique** pour de nombreuses entreprises. Elle se décline en trois volets : **la gestion des infrastructures** (serveurs, réseaux, bases de données), **la gestion des applications** (maintenance et support), et **l'hébergement de services** (sites web, applications métiers). En 2021, ce marché représentait **31,6 milliards de dollars à l'échelle mondiale**, avec une **croissance annuelle moyenne de 8%**. Toutefois, cette externalisation ne signifie pas un désengagement interne : **77% des RSSI déclarent y recourir**, mais **89% des décisions stratégiques en matière de sécurité restent prises en interne**. L'internalisation permet notamment de maintenir une **veille technologique active** et de **sensibiliser les équipes**, tandis que l'externalisation assure une **surveillance continue 24/7** par des experts. Pour garantir un appel d'offre sécurisé, **l'ANSSI recommande** de bien **définir les besoins**, d'**évaluer les offres selon des critères multiples**, et de **vérifier la conformité réglementaire des prestataires**.

Ces quatre enjeux illustrent à quel point la cybersécurité dépasse le simple cadre technique. Elle touche directement à la stratégie, à la réputation et à la stabilité des organisations. Bien entendu, d'autres enjeux existent, comme la conformité réglementaire, la protection de la vie privée ou encore la gestion des identités. Tous méritent une attention particulière dans une approche globale de la sécurité numérique.

2.2.3 Lien entre Cybersécurité et Performance Durable

Dans le contexte du reporting de durabilité promu par la CSRD, la cybersécurité tend à dépasser son rôle purement technique pour devenir un enjeu stratégique transversal, directement lié à la performance durable des organisations. Loin de se limiter à une question d'infrastructure ou de conformité, elle s'inscrit aujourd'hui dans une logique de responsabilité sociétale, incarnée notamment par les piliers que sont **l'environnement**, **le social** et **l'économie** - trois dimensions clés de la durabilité moderne.

Pilier n°1 - La cybersécurité et l'environnement

La cybersécurité contribue à la réduction de l'impact environnemental du numérique en favorisant une gestion plus efficiente des infrastructures informatiques :

- En limitant les interruptions de service et les pertes de données, elle évite des redémarrages massifs de serveurs ou des reconstructions de systèmes, qui sont énergivores.
- Elle s'inscrit dans une démarche de numérique responsable, en lien avec la transition écologique, en optimisant les ressources numériques et en réduisant l'empreinte carbone des systèmes d'information [37].

Pilier n°2 - La cybersécurité et le social

La cybersécurité protège les droits fondamentaux des individus et renforce la confiance au sein de l'organisation :

- Elle garantit la confidentialité des données personnelles des parties prenantes.
- Elle contribue à un environnement de travail sain et sécurisé, en luttant contre les risques de harcèlement numérique ou de manipulation.
- Elle participe à la sensibilisation et à la formation des collaborateurs, renforçant ainsi la culture de sécurité et la responsabilité collective [26].

Pilier n°3 - La cybersécurité et l'économie

La cybersécurité est un levier de performance durable :

- Elle protège les actifs numériques, la propriété intellectuelle et les processus critiques de l'entreprise.
- Elle limite les pertes financières liées aux cyberattaques.
- Elle renforce la confiance des parties prenantes (clients, investisseurs, partenaires), ce qui est essentiel à la pérennité économique de l'entreprise [27].

Ces liens montrent que la cybersécurité ne relève plus uniquement de la technique, mais s'inscrit pleinement dans une stratégie RSE globale, en cohérence avec les attentes réglementaires et sociétales actuelles.

3 La Cybersécurité dans les référentiels de durabilité

Alors que la cybersécurité s'impose comme un enjeu stratégique pour les entreprises, sa reconnaissance explicite dans les référentiels de durabilité reste encore inégale. Pourtant, les cyberattaques peuvent avoir des impacts majeurs sur la continuité d'activité, la confidentialité des données, la réputation des entreprises et, plus largement, sur les parties prenantes. Cette section vise à dresser un état des lieux de l'intégration de la cybersécurité dans les principaux cadres de reporting en matière de durabilité, en mettant en lumière les normes européennes (ESRS), les standards internationaux (GRI, SASB, ISO, etc.), les approches de double matérialité, ainsi que les types de données attendues dans les rapports ESG.

3.1 Introduction à la cybersécurité dans le contexte ESG

La cybersécurité, longtemps considérée comme affaire purement technique, devient aujourd'hui un enjeu de gouvernance, de résilience et de durabilité pour les organisations publiques et privées. Dans un monde numérisé, les cyberattaques ne se limitent plus à des incidents isolés mais peuvent perturber fortement les opérations critiques, détériorer la confiance des parties prenantes et engendrer des conséquences socio-économiques majeures.

Un exemple récent : Brussels Airport, en septembre 2025, a subi une cyberattaque via un fournisseur externe (Collins Aerospace) qui a paralysé ses systèmes de check-in et d'embarquement automatiques [1]. L'aéroport a dû recourir à des processus manuels, annuler ou détourner plusieurs vols (ex. 44 départs ou redirections) et accélérer le déploiement d'un nouveau système, prévu à l'origine pour novembre, pour rétablir ses capacités [4].

Autre cas belge : le Service public de Wallonie (SPW) victime d'une intrusion importante en avril 2025. Le SPW a dû couper ses connexions Internet, rendre inaccessibles beaucoup d' applications, d'ordinateurs et de serveurs, suspendre certains services publics numériques, et prolonger les délais administratifs pour compenser ces perturbations [45].

Ces exemples illustrent que la cybersécurité touche directement les volets Gouvernance (G) et Social (S) des critères ESG : transparence, responsabilité, continuité opérationnelle, protection des données et de l'accès aux services.

L'intégration de la cybersécurité dans les rapports de durabilité n'est plus une option mais une nécessité, à la fois pour informer les investisseurs et les régulateurs sur les capacités de gestion de ces risques numériques, et pour préserver la confiance des citoyens, des usagers, des employés.

Avec la CSRD (Corporate Sustainability Reporting Directive), l'approche de la double matérialité pourrait constituer une base solide pour intégrer plus concrètement la cybersécurité dans les pratiques de reporting durable. Au-delà de l'évaluation des risques numériques, la CSRD offrirait un cadre pertinent pour y inclure des indicateurs relatifs à la sécurité des systèmes d'information, à la gouvernance des données, ou encore à la sensibilisation des collaborateurs.

3.2 Analyse des ESRS (European Sustainability Reporting Standards)

La mise en œuvre de la CSRD s'accompagne des ESRS (European Sustainability Reporting Standards). Ces normes définissent les exigences de divulgation ESG pour les entreprises européennes. Elles offrent un cadre structuré pour le reporting de durabilité. La cybersécurité peut y être intégrée, mais les mentions explicites restent limitées.

3.3 Cybersécurité dans les normes transversales (ESRS 1 et ESRS 2)

Les standards généraux (ESRS 1 et ESRS 2) posent les bases du reporting ESG. Ils imposent des exigences sur la gouvernance, la stratégie et la gestion des impacts, risques et opportunités (IRO). La cybersécurité peut y être intégrée de manière implicite. Par exemple, elle peut apparaître dans la supervision des risques par la direction, la gestion des vulnérabilités dans la chaîne de valeur ou l'identification des risques matériels affectant la performance et la résilience de l'entreprise.

Les ESRS 1 et 2 n'utilisent pas toujours le terme "cybersécurité", mais ils introduisent plusieurs concepts où elle peut s'inscrire. Les entreprises doivent décrire leurs structures de gouvernance liées à la durabilité. Elles doivent expliquer comment elles identifient les impacts, risques et opportunités. Elles doivent aussi présenter les politiques mises en œuvre et les indicateurs de performance associés. Ces exigences permettent d'inclure des éléments tels que les politiques de cybersécurité, le taux d'incidents, les résultats d'audits ou la formation du personnel.

Pour être précis, les standards incluent ESRS 2-GOV et ESRS 2-RSK (gouvernance et gestion des risques), ESRS 2-IRO (processus de double matérialité) et ESRS 2-SBM (politiques et

indicateurs). Ces éléments offrent des points d'ancrage clairs pour intégrer la cybersécurité dans le reporting ESG.

Cependant, les mentions explicites de la cybersécurité restent rares dans les ESRS actuels. Les prescriptions sectorielles détaillant ces enjeux sont peu développées. De plus, seule une minorité d'entreprises publie des informations spécifiques sur la cybersécurité ou la protection des données, souvent via des "entity-specific disclosures" [35, 43].

Ces constats suggèrent que les ESRS pourraient servir de cadre pour une intégration plus systématique de la cybersécurité. Des exigences explicites pourraient inclure des indicateurs sur la gouvernance des incidents cyber, la résilience des systèmes d'information, la formation du personnel ou la conformité à des standards comme ISO 27001 ou NIST. Une telle approche renforcerait la transparence, la confiance et la résilience des organisations face aux enjeux numériques, tout en complétant le reporting ESG existant.

3.3.1 Cybersécurité dans les normes thématiques (ESRS S et G)

Les normes thématiques ESRS S (Social) et G (Governance) offrent un cadre plus spécifique pour intégrer la cybersécurité dans le reporting ESG des entreprises.

ESRS S1 – Personnel de l'entreprise [10]

La cybersécurité peut être abordée sous l'angle de la protection des données personnelles des employés, de la formation à la sécurité numérique, ou encore de la prévention des risques psychosociaux liés aux cyberattaques (ex. : phishing, harcèlement numérique).

ESRS G1 – Conduite des affaires [9]

Cette norme couvre les politiques de conformité, d'éthique et de lutte contre la corruption. La cybersécurité y trouve sa place à travers la gestion des accès, la protection des données sensibles, et la prévention des fraudes numériques.

3.3.2 Cybersécurité dans les normes sectorielles (à venir)

Les normes sectorielles ESRS, actuellement en cours d'élaboration, devraient permettre une intégration plus fine de la cybersécurité, en particulier dans les secteurs à forte exposition

numérique tels que la finance, la santé et les télécommunications. Ces normes visent à préciser les enjeux spécifiques à chaque secteur, afin de compléter les normes transversales ESRS 1 et 2. Cependant, leur adoption a été reportée au 30 juin 2026, conformément à la décision du Parlement européen du 17 avril 2024 [31].

Dans ce contexte, on peut s'attendre à ce que des exigences spécifiques apparaissent concernant :

- La gestion des incidents de sécurité informatique : les entreprises devront mettre en place des procédures de notification rapide des incidents, conformément aux obligations de la directive NIS 2 [46].
- La résilience des systèmes critiques : les entités essentielles et importantes devront assurer la continuité de leurs opérations en cas d'incident majeur, en mettant en place des plans de gestion des crises et de reprise après sinistre [46].
- La conformité aux standards techniques : les entreprises devront se conformer à des normes reconnues telles que l'ISO 27001 ou la directive NIS 2, qui imposent des exigences strictes en matière de cybersécurité [46].

Il est à noter que le règlement DORA (Digital Operational Resilience Act), adopté en 2022, impose déjà des exigences spécifiques en matière de résilience opérationnelle numérique pour le secteur financier, notamment la gestion des risques liés aux technologies de l'information et de la communication (TIC).

En conclusion, bien que les normes sectorielles ESRS ne soient pas encore finalisées, les évolutions réglementaires en cours témoignent d'une volonté d'intégrer de manière plus précise la cybersécurité dans le reporting ESG des entreprises, en particulier dans les secteurs à forte exposition numérique.

3.3.3 Limites actuelles et perspectives

À ce jour, la cybersécurité n'est pas encore traitée comme un thème autonome dans les ESRS, contrairement à des sujets comme le climat ou la biodiversité. Toutefois, son intégration implicite dans les dimensions de gouvernance, de gestion des risques et de protection des données laisse entrevoir une évolution possible vers une reconnaissance plus explicite. L'alignement avec d'autres cadres internationaux (GRI, SASB, etc.) pourrait également renforcer cette tendance.

3.4 Comparaison avec d'autres standards internationaux (GRI, SASB, SEC, ISO, etc.)

Les **ESRS** sont le socle réglementaire européen pour le reporting de durabilité. Mais d'autres standards internationaux influencent aussi les pratiques des entreprises, surtout celles présentes dans plusieurs juridictions. La cybersécurité y est de plus en plus considérée comme un **enjeu ESG**, notamment pour la gouvernance et le volet social.

Le **GRI (Global Reporting Initiative)** propose des lignes directrices générales sur la gestion des risques et la protection des données personnelles. Il recommande de divulguer les politiques et les incidents significatifs, mais reste peu prescriptif sur les mesures techniques.

Le **SASB (Sustainability Accounting Standards Board)** adopte une approche sectorielle. Certaines industries doivent détailler la gestion des incidents, la protection des données et la résilience des systèmes d'information. SASB est donc plus précis que le GRI pour les risques propres à chaque secteur.

La **SEC (Securities and Exchange Commission)** aux États-Unis exige la divulgation des cyberincidents significatifs et des pratiques de gestion des risques. Elle met l'accent sur la transparence et l'impact des incidents sur la performance financière.

Les **standards techniques** comme **ISO 27001** ou la directive européenne **NIS2** ne sont pas des standards ESG à proprement parler. Ils fournissent un cadre pour sécuriser et rendre résilients les systèmes d'information. Ils servent de guide pratique pour mettre en œuvre les exigences ESG liées à la cybersécurité.

En résumé, ces standards se rejoignent sur la nécessité d'une **bonne gouvernance et d'une gestion des incidents**. Ils diffèrent surtout par la **granularité et l'approche sectorielle**. Cette section introduit les principaux cadres qui seront détaillés dans les parties suivantes.

3.4.1 GRI (Global Reporting Initiative)

Le **GRI (Global Reporting Initiative)** est l'un des standards de reporting de durabilité les plus utilisés au monde. Il est adopté par plus de 10.000 organisations dans plus de 100 pays [53]. Son objectif est d'aider les entreprises à rendre compte de leurs impacts sur l'économie, l'environ-

nement et la société. Le GRI met l'accent sur la transparence et la responsabilité.

Le GRI ne dispose pas d'une norme spécifique pour la cybersécurité. Toutefois, il aborde indirectement la question à travers la norme **GRI 418 – Confidentialité des données**. Cette norme se concentre sur la protection des informations personnelles des clients, un aspect clé de la cybersécurité. Elle demande aux entreprises de divulguer le nombre de plaintes fondées concernant des violations de la vie privée ou des pertes de données. Elle exige aussi de présenter les mesures prises pour gérer ces incidents, notamment les politiques et mécanismes de contrôle en matière de confidentialité [28].

Le GRI présente néanmoins certaines limites pour la cybersécurité. Il adopte une approche centrée sur les impacts externes (inside-out), c'est-à-dire qu'il se concentre sur les effets sur les parties prenantes. Les risques internes, comme l'impact financier d'une cyberattaque, sont peu pris en compte. De plus, le GRI ne fournit pas de directives sectorielles précises, ce qui limite la pertinence des informations pour les secteurs à forte exposition numérique. Enfin, il ne propose pas de normes techniques comme ISO 27001 pour guider la mise en œuvre opérationnelle de la cybersécurité.

Pour répondre à ces défis, le GRI a commencé à réviser ses standards. Un rapport publié en septembre 2024 identifie les lacunes existantes et propose de mieux intégrer les impacts numériques, y compris ceux liés à la cybersécurité [29]. Cela montre une évolution vers un traitement plus concret de la cybersécurité dans le reporting ESG.

3.4.2 SASB (Sustainability Accounting Standards Board)

Le **SASB (Sustainability Accounting Standards Board)** est une organisation à but non lucratif fondée en 2011. Elle développe des normes de divulgation spécifiques à chaque secteur, visant à aider les entreprises à communiquer sur les risques et opportunités ESG pertinents pour les investisseurs [49].

Le SASB aborde la cybersécurité principalement à travers le standard **TC-SI-230a** [12], dédié aux entreprises du secteur technologique et des communications. Ce standard exige des entreprises qu'elles divulguent :

- Leur approche pour identifier et traiter les vulnérabilités dans leurs systèmes d'information.
- Les procédures opérationnelles, les processus de gestion, la structure des produits, la sélection des partenaires commerciaux, la formation des employés et l'utilisation de la technologie pour gérer les risques de sécurité des données.
- Leur utilisation de normes de gestion des risques de cybersécurité tierces.
- Les tendances observées en termes de types, de fréquence et d'origine des attaques contre la sécurité des données et des systèmes d'information.

Ces exigences visent à fournir aux investisseurs des informations sur la manière dont les entreprises gèrent les risques liés à la cybersécurité et à évaluer l'impact potentiel de ces risques sur la performance financière.

Le SASB adopte une approche sectorielle, reconnaissant que les risques et opportunités liés à la cybersécurité varient selon les industries. Par exemple, les entreprises du secteur technologique sont tenues de divulguer des informations plus détaillées sur la cybersécurité que celles d'autres secteurs. Cette approche permet une évaluation plus précise des risques spécifiques à chaque secteur.

Cependant, le SASB présente certaines limites. Il ne fournit pas de directives spécifiques sur la manière de mettre en œuvre les mesures de cybersécurité, laissant aux entreprises le soin de déterminer les pratiques appropriées. De plus, bien que le SASB mette l'accent sur la transparence, il ne prescrit pas de normes techniques détaillées, telles que celles proposées par ISO 27001, pour la gestion de la cybersécurité.

En résumé, le SASB offre un cadre utile pour la divulgation des risques liés à la cybersécurité, en particulier pour les entreprises des secteurs technologique et des communications. Toutefois, il existe des opportunités pour renforcer ce cadre, notamment en intégrant des normes techniques spécifiques et en fournissant des directives plus détaillées sur la mise en œuvre des pratiques de cybersécurité.

3.4.3 SEC (Securities and Exchange Commission – États-Unis)

La **Securities and Exchange Commission (SEC)** est l'autorité américaine chargée de réguler les marchés financiers. Elle supervise les entreprises cotées pour garantir la transparence et protéger les investisseurs. La SEC établit des règles de divulgation, notamment sur les risques financiers et opérationnels [48].

Depuis juillet 2023, la SEC a renforcé les obligations de reporting liées à la cybersécurité. L'objectif est de fournir aux investisseurs des informations fiables et comparables sur la gestion des risques cyber, la stratégie et la gouvernance des entreprises.

Une des principales exigences concerne la divulgation rapide des incidents de cybersécurité jugés "matériels". Les entreprises doivent les déclarer via le **Form 8-K, Item 1.05**, dans un délai de quatre jours ouvrables après avoir déterminé leur matérialité. Ces déclarations doivent préciser la nature, l'étendue et le calendrier de l'incident, ainsi que son impact ou son impact probable sur l'entreprise [47].

La Regulation **S-K, Item 106** impose également aux entreprises de divulguer annuellement leurs processus pour évaluer, identifier et gérer les risques cyber. Elles doivent détailler le rôle de la direction et du conseil d'administration dans la supervision de ces risques, ainsi que les politiques et procédures mises en place pour les gérer [47].

Ces nouvelles règles améliorent la transparence et la comparabilité des informations sur la cybersécurité. Elles aident les investisseurs à évaluer les risques et les opportunités associés aux entreprises. Les règles sont entrées en vigueur le 18 décembre 2023 pour la plupart des entreprises, avec une date limite de conformité pour les petites entreprises fixée au 15 juin 2024 [36].

3.4.4 ISO 27001 et autres normes techniques

La norme **ISO/IEC 27001 :2022** est une référence majeure pour la cybersécurité. Elle définit les exigences pour créer, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (SMSI). ISO 27001 repose sur une approche basée sur les risques. Elle permet aux organisations d'identifier, d'évaluer et de traiter les menaces sur la confidentialité,

l'intégrité et la disponibilité des informations. La norme inclut la gouvernance, la gestion des incidents, la formation du personnel et la conformité légale. Elle est reconnue à l'international et sert de socle pour démontrer l'engagement en cybersécurité [32].

D'autres cadres techniques complètent ISO 27001. Le **NIST Cybersecurity Framework (CSF 2.0)** propose six fonctions : **Gouverner**, **Identifier**, **Protéger**, **Détecter**, **Répondre** et **Récupérer**. Il met l'accent sur la gouvernance stratégique, la gestion des risques et la résilience des systèmes critiques. Le NIST CSF 2.0 permet aussi de définir des profils cibles et d'évaluer les écarts, ce qui aide à planifier les améliorations et prioriser les actions [39].

D'autres normes et directives viennent compléter ce cadre. **ISO/IEC 27002** donne des bonnes pratiques pour les contrôles de sécurité. La directive européenne **NIS2** [42] impose des exigences aux opérateurs d'infrastructures critiques et aux fournisseurs de services numériques. Elle insiste sur la gestion des incidents, la protection des systèmes essentiels et la coopération entre États. Enfin, **COBIT** [34] propose une approche de gouvernance et de management des technologies de l'information. Il couvre la gestion des risques, le contrôle interne et le reporting stratégique. Ensemble, ces standards permettent de structurer la cybersécurité, de renforcer la résilience et de répondre aux exigences ESG en matière de sécurité numérique.

3.4.5 ESG Ratings et agences de notation

Les agences de notation ESG, telles que **MSCI** et **Sustainalytics**, intègrent la cybersécurité dans leurs évaluations, principalement sous l'angle de la gouvernance des risques. Chez MSCI, la **cybersécurité et la confidentialité des données** sont considérées comme des enjeux clés dans le pilier social de leur modèle ESG. Les entreprises sont évaluées en fonction de leur exposition aux risques liés à la collecte de données personnelles, à leur vulnérabilité aux violations de données et à la gestion de la conformité aux réglementations en évolution. La note attribuée combine une évaluation de l'exposition et de la gestion des risques, avec des scores allant de 0 à 10, où un score élevé indique une gestion robuste des risques [38].

De son côté, Sustainalytics considère la **cybersécurité et la confidentialité des données** comme une question ESG matérielle majeure. L'agence évalue l'exposition des entreprises à ces risques

en fonction de leur secteur d'activité et de leur modèle commercial. Elle examine également la gestion de ces risques, en tenant compte des politiques internes, des audits de sécurité et des réponses aux incidents [50].

Cependant, les méthodologies varient d'une agence à l'autre, ce qui peut limiter la comparabilité des évaluations. Par exemple, la pondération accordée à la cybersécurité dans le score ESG global peut différer selon les secteurs et les priorités stratégiques de chaque agence. Cela souligne l'importance pour les entreprises de comprendre les critères spécifiques utilisés par chaque agence et d'adopter des pratiques de cybersécurité transparentes et alignées sur les meilleures pratiques du secteur.

3.4.6 Synthèse comparative Conclusion

L'analyse comparative des principaux cadres et standards internationaux, **présentée dans le tableau de synthèse à la page suivante**, met en évidence une réalité claire : il n'existe pas encore, à l'échelle européenne, de document **contraignant**, clair et complet intégrant de manière précise la cybersécurité dans le reporting de durabilité. Les référentiels existants sont souvent **soit non contraignants**, comme l'ISO 27001, le NIST ou le COBIT, **soit limités à certains secteurs d'activité**, comme le SASB ou la directive NIS2, qui ciblent principalement les infrastructures critiques et les services numériques. D'autres cadres, tels que le GRI, la SEC ou les notations ESG (MSCI, Sustainalytics), se concentrent avant tout sur la transparence et la gouvernance, sans offrir de cadre opérationnel complet.

En conséquence, il n'existe pas aujourd'hui de norme **européenne** qui combine à la fois les dimensions **techniques**, **stratégiques** et **de reporting**, tout en étant applicable de manière transversale et auditable. Les initiatives comme la **CSRD** et les **ESRS** posent des bases importantes, mais elles demeurent trop générales sur le plan cyber : les exigences explicites manquent, les indicateurs restent à définir, et la comparabilité entre entreprises est encore faible.

L'objectif n'est pas de complexifier davantage un paysage déjà dense, mais de **compléter la CSRD** par des éléments **concrets**, **vérifiables** et, à terme, **contraignants** liés à la cybersécurité-tels que la gouvernance des incidents, la formation des employés, la résilience des systèmes

d'information ou la conformité à des standards reconnus (ISO 27001, NIST, NIS2). Une telle évolution permettrait d'assurer une meilleure lisibilité du reporting, de renforcer la confiance des parties prenantes, et de préparer les organisations européennes aux **défis numériques et réglementaires** à venir.

Pour illustrer concrètement ces enjeux, la section suivante se concentre sur une **analyse pratique de rapports réels publiés par des entreprises dans le cadre de la CSRD**. L'objectif est d'examiner **ce qui est effectivement communiqué au sujet de la cybersécurité**, de la gouvernance des systèmes d'information à la résilience opérationnelle, afin de mettre en lumière les **écarts éventuels entre les exigences théoriques et la réalité du reporting**. Cette approche permettra de **passer de la théorie à la pratique**, en identifiant les bonnes pratiques déjà adoptées par certaines organisations et les domaines où des améliorations sont nécessaires pour renforcer la transparence et la fiabilité des informations publiées.

Standard / Cadre	Contraignant / Volontaire	Cible	Secteur d'activité	Objectif principal	Cybersécurité incluse	Approche
ISO/IEC 27001	Volontaire / certifiable	Toutes organisations	Tous secteurs	Gestion et amélioration d'un SMSI (sécurité de l'information)	Oui, via contrôle des risques, gouvernance, incidents, formation	Basée sur les risques, management, contrôles techniques et organisationnels
NIS2	Contraignant (UE)	Opérateurs d'infrastructures critiques et fournisseurs de services numériques	Énergie, transport, santé, finance, numérique	Renforcer la cybersécurité des systèmes essentiels	Oui, exigences détaillées sur gestion incidents, résilience, audits	Réglementaire, obligations légales, reporting aux autorités
COBIT	Volontaire	Toutes organisations	Tous secteurs	Gouvernance et management des TI	Oui, intégrée à la gouvernance IT et aux risques	Processus et objectifs de contrôle, alignement stratégie IT/cybersécurité
NIST CSF	Volontaire	Toutes organisations	Tous secteurs, surtout USA	Gestion des risques cyber et amélioration continue	Oui, structure complète : Identifier, Protéger, Détecter, Répondre, Récupérer	Basée sur fonctions et profils, flexible et adaptable
MSCI ESG Ratings	Volontaire	Investisseurs et entreprises	Tous secteurs	Évaluation ESG pour investisseurs	Oui, dans gouvernance des risques et protection des données	Notation basée sur exposition et gestion des risques cyber
Sustainalytics ESG Ratings	Volontaire	Investisseurs et entreprises	Tous secteurs	Évaluation ESG, matérialité sectorielle	Oui, cybersécurité et confidentialité des données évaluées	Scoring basé sur exposition et gestion, audits et incidents
SEC (US)	Contraignant	Entreprises cotées US	Tous secteurs	Transparence et divulgation des risques cyber	Oui, via Form 8-K Item 1.05 et Regulation S-K Item 106	Reporting légal obligatoire sur incidents et gouvernance cyber
GRI	Volontaire	Toutes organisations	Tous secteurs	Reporting ESG / durabilité	Oui, indirectement via GRI 418 (confidentialité des données)	Focus impacts externes (inside-out), peu technique
SASB	Volontaire	Entreprises et investisseurs	Sectoriel (plus détaillé pour tech, communications)	Reporting ESG financier et sectoriel	Oui, via standards sectoriels (ex. TC-SI-230a)	Approche sectorielle, centrée sur risques et divulgation aux investisseurs

FIGURE 1 – Tableau de synthèse des principaux cadres et standards internationaux

4 Étude de cas : Analyse de rapports CSRD récents

Cette étude cherche à comprendre comment la **cybersécurité** apparaît aujourd'hui dans les rapports de durabilité publiés par les grandes entreprises européennes. Après avoir analysé les **cadres théoriques et réglementaires** comme la **CSRD** et les **ESRS**, nous avons également examiné les **principaux référentiels et standards existants** traitant du reporting cyber (ISO 27001, NIST, GRI, SASB, etc.). Cette première analyse a montré que, même si ces cadres apportent des éléments utiles, aucun ne propose un dispositif contraignant, clair et transversal pour intégrer la cybersécurité dans le reporting de durabilité. Ces référentiels sont souvent partiels, sectoriels ou non vérifiables. C'est précisément ce manque que cette étude de terrain cherche à mieux comprendre.

L'objectif est donc d'observer la **réalité du terrain** : comment les entreprises traduisent concrètement les exigences de durabilité dans leurs pratiques, et quelle place elles accordent à la sécurité numérique dans ce cadre.

4.1 Méthodologie de l'étude

Le corpus comprend **trois grandes entreprises européennes**, choisies pour représenter des **secteurs variés** et des **niveaux de maturité différents** face aux risques cyber :

- **TotalEnergies** (Énergie) - Représente un secteur à infrastructures critiques fortement numérisées (IT/OT), où la continuité d'activité et la sécurité industrielle rendent le risque cyber structurant pour la gouvernance et la résilience.
- **BNP Paribas** (Finance) - Illustratif d'un environnement hautement régulé (RGPD, DORA) avec forte exposition aux données sensibles et aux paiements digitaux, donc pertinent pour évaluer la maturité du pilotage et du reporting cyber.
- **Airbus** (Industrie/Défense) - Acteur stratégique soumis à des menaces avancées (chaîne d'approvisionnement, propriété intellectuelle, contexte géopolitique), utile pour observer l'intégration du cyber dans le risque d'entreprise et la souveraineté technologique.

Ces entreprises font partie des premières concernées par l'application de la **CSRD**. Leur analyse permet d'observer comment les pionniers du reporting extra-financier intègrent la cybersécurité dans leur communication et leur gouvernance. Le choix de secteurs différents aide aussi à

identifier les **écarts de maturité** et les **bonnes pratiques émergentes**.

La **méthodologie** repose sur une lecture **qualitative et comparative** des rapports publiés pour l'année **2024**, période charnière de mise en conformité avec la CSRD. Les documents étudiés incluent des **rapports de durabilité dédiés** et des **rapports intégrés** combinant performance financière et extra-financière.

L'analyse s'appuie sur une grille de critères inspirée des ESRS et des principaux standards de cybersécurité :

- **Intégration dans la gouvernance** : Regroupe la place de la cybersécurité dans les instances de décision (Conseil, Comex, CISO), son lien avec la stratégie d'entreprise et la gestion des risques (ERM/ESRS). Évalue qui décide, comment c'est piloté et comment le sujet irrigue les priorités ESG.
- **Organisation opérationnelle** : Couvre l'appareil "terrain" : équipes, rôles, politiques, et contrôles déployés (SOC, CERT, IAM/MFA, chiffrement, segmentation, gestion des vulnérabilités, formation). Mesure la capacité concrète à prévenir, détecter et répondre aux incidents (IT/OT).
- **Suivi, audit et indicateurs** : Porte sur le contrôle interne, les audits (internes/externes), et les KPI publiés (incidents, délais de détection/réponse, couverture de formation, conformité). Juge le niveau de transparence, d'objectivité et de comparabilité du reporting.

Cette approche permet de mesurer non seulement la présence du thème dans les rapports, mais aussi la **profondeur de son traitement**. Elle vise à mieux comprendre pourquoi la cybersécurité reste encore **inégalement intégrée** dans les démarches de durabilité, et comment elle pourrait être mieux **ancrée dans les futurs standards européens**.

4.2 Analyse des rapports

L'analyse des rapports CSRD ou de durabilité publiés par **TotalEnergies**, **Airbus** et **BNP Paribas** permet d'observer comment des entreprises européennes majeures, issues de secteurs variés, abordent la cybersécurité dans leur communication extra-financière. Ces organisations figurent parmi les premières concernées par la CSRD, ce qui en fait un échantillon pertinent pour évaluer la maturité actuelle du reporting cyber.

Information

Les informations suivantes sont principalement extraites du document de référence officiel, tel que publié sur les sites officiels des différentes entreprises.

— TotalEnergies - Document d'enregistrement universel 2024 [52]

— Airbus - Annual Report 2024 [3]

— BNP Paribas - Rapport intégré [6] & Document d'enregistrement universel 2024 [7]

4.2.1 TotalEnergies

TotalEnergies est un leader mondial du secteur énergétique, présent dans plus de 130 pays. Ses activités couvrent l'exploration, la production, le raffinage et la distribution d'énergie. Le groupe est fortement exposé aux risques cyber, notamment en raison de la numérisation de ses infrastructures industrielles et de la gestion de données sensibles. Cette exposition rend la cybersécurité critique pour la continuité des opérations et la protection des actifs stratégiques [51].

Gouvernance et stratégie

La cybersécurité occupe une place centrale dans la gouvernance de TotalEnergies. Le rapport indique que « les enjeux de cybersécurité font l'objet d'un engagement fort de la Direction générale » (p. 148). Le dispositif est supervisé par plusieurs instances clés : le TotalEnergies Risk Management Committee (TRMC), le Comité exécutif (Comex) et le Comité d'audit. Le Directeur financier, membre du Comex, supervise directement la direction des systèmes d'information, au sein de laquelle le Global Chief Information Security Officer (CISO) pilote la stratégie cyber.

Chaque année, la Direction Cybersécurité & Management des Risques soumet au Comex une stratégie de cybersécurité couvrant les systèmes d'information industriels et d'entreprise. Celle-ci est validée par le Comité d'audit puis présentée au Conseil d'administration. Cette gouvernance structurée traduit une volonté d'inscrire la cybersécurité dans une logique de pilotage stratégique et transversal. Le rapport souligne que la stratégie « définit les évolutions du référentiel cybersécurité de la Compagnie » (p. 148), en cohérence avec

- les objectifs ESG et les orientations de la CSRD.

Organisation opérationnelle et mesures de protection

Sur le plan opérationnel, TotalEnergies déploie une organisation robuste articulée autour d'un Centre opérationnel de sécurité (SOC) et d'un Computer Emergency Response Team (CERT) certifié FIRST et TF-CSIRT. Ce dispositif assure la détection, l'analyse et la réponse aux incidents de sécurité. Le rapport indique qu'en 2024, « plusieurs millions d'attaques ont été bloquées par les systèmes de défense informatique de la Compagnie et plusieurs milliers ont nécessité l'intervention des équipes techniques » (p. 137).

L'entreprise applique une approche basée sur la défense en profondeur, intégrant la segmentation des réseaux, la supervision continue, la gestion des vulnérabilités et la formation du personnel. La direction cybersécurité élabore et diffuse des règles de gouvernance et de sécurité détaillant les infrastructures, les organisations et les modes opératoires. Celles-ci sont déployées dans toutes les filiales et adaptées à leurs risques spécifiques.

Les actions de sensibilisation sont un pilier important : TotalEnergies organise chaque année un « Mois de la cybersécurité » et des campagnes de prévention contre le phishing. Des formations obligatoires et des modules spécifiques par fonction complètent ce dispositif, contribuant à développer une véritable culture cyber au sein du groupe (p. 409).

Suivi, audit et indicateurs

Le suivi du dispositif cyber repose sur une combinaison d'audits internes, d'autoévaluations et de contrôles externes. Le Comité d'audit supervise la mise en œuvre du programme, examine régulièrement « les résultats des missions d'audit conduites, les autoévaluations et, si nécessaire, tout incident de cybersécurité significatif » (p. 409). Les informations sont ensuite consolidées et remontées au Conseil d'administration.

TotalEnergies a également mis en place des analyses de risques spécifiques pour définir les contrôles appropriés et tester la résilience de ses systèmes. Ces contrôles reposent sur le principe des trois lignes de défense : la supervision opérationnelle, les fonctions de contrôle interne, et les audits indépendants menés par la direction Sûreté. Celle-ci réalise

chaque année plusieurs simulations d'attaques ("red team") avec des prestataires externes spécialisés, ainsi que des exercices de gestion de crise cyber (p. 148).

Cette approche proactive permet à l'entreprise de mesurer et d'améliorer en continu la maturité de son dispositif cyber, bien que peu d'indicateurs chiffrés soient publiés dans le rapport.

Alignement ESRS 2- GOV / RSK / IRO / SBM (et DC-M / DC-T)

Gouvernance (ESRS 2 GOV-1/2/5). Le *Document d'enregistrement universel 2024* inscrit la cybersécurité dans le rapport du Conseil et le dispositif de contrôle interne, avec rôles, supervision par les comités et assurance du reporting. Cela couvre l'organisation, la responsabilité et la revue par le Conseil attendues par ESRS 2.

Risques (ESRS 2 RSK-1). La cartographie des risques et les dispositifs de maîtrise intègrent le risque cyber (IT/OT, tiers, données). Les processus d'identification, d'évaluation et de mitigation décrits satisfont les exigences RSK-1 (méthodes, périmètre, fréquence des revues).

Matérialité et stratégie (ESRS 2 IRO-1/2 et SBM-3). La publication au titre CSRD implique une double matérialité et l'intégration de la cybersécurité à la stratégie et au modèle d'affaires (impacts, risques, opportunités, dépendances critiques), conformément à IRO et SBM.

Indicateurs publiables (DC-M / DC-T). Exemples alignés ESRS 2 : *existence d'une politique cyber approuvée*, *définition et nombre d'incidents significatifs*, *délais de détection/réponse* (MTTD/MTTR), *taux de formation/sensibilisation*, *périmètre de certification ISO 27001* et *avancement des plans de remédiation*.

Notes : ESRS 2 = exigences générales (GOV : gouvernance, RSK : risques, IRO : impacts / risques / opportunités, SBM : modèle d'affaires / stratégie). DC-M / DC-T = divulgations « Metrics » / « Targets/Tests » pour rendre l'information mesurable et comparable.

En conclusion, TotalEnergies présente un modèle de gouvernance cyber parmi les plus struc-

turés du secteur de l'énergie. L'entreprise relie explicitement la cybersécurité à la résilience opérationnelle, à la conformité réglementaire et à la confiance des parties prenantes. L'existence d'une stratégie approuvée par le Comex, d'un CERT certifié internationalement et d'exercices réguliers de simulation illustre un haut niveau de maturité.

Cependant, le reporting cyber demeure principalement qualitatif. Les indicateurs de performance et de suivi restent internes, sans publication standardisée ou audit externe systématique. Cette limite confirme la nécessité d'un cadre européen plus contraignant et homogène, afin d'intégrer pleinement la cybersécurité dans la durabilité d'entreprise au sens de la CSRD.

4.2.2 Airbus

Airbus est un leader mondial de l'aéronautique, de la défense et du spatial. L'entreprise emploie plus de 157 000 personnes et opère dans un environnement hautement technologique et sensible. La cybersécurité représente un risque stratégique majeur, compte tenu de la complexité de ses chaînes d'approvisionnement et des menaces géopolitiques qui pèsent sur son secteur [2].

Gouvernance et stratégie

Airbus place la cybersécurité au cœur de sa gouvernance stratégique. La direction a identifié ce risque comme un enjeu critique pour la résilience du groupe, au même titre que la sûreté industrielle ou la conformité réglementaire. Le rapport précise que « le risque de matérialisation d'une cyberattaque, incluant intrusion dans les systèmes, perte de données ou atteinte à la résilience industrielle, pourrait entraîner des pertes financières importantes et une dégradation de la réputation » (p. 67).

La cybersécurité est supervisée par la Group Cyber Review Board, une instance permanente présidée par le Corporate Chief Information Security Officer (CISO) et composée des responsables cybersécurité de chaque division : Commercial Aircraft, Helicopters et Defence & Space. Ce comité se réunit chaque trimestre pour « examiner les risques, discuter des vulnérabilités et convenir d'actions de mitigation à l'échelle du groupe » (p. 211). Cette approche transversale renforce la cohérence stratégique et garantit que les enjeux cyber sont intégrés dans toutes les entités du groupe.

Airbus a également déployé une stratégie cybersécurité triennale (2023-2025), révisée régulièrement « en fonction de l'évolution des menaces et du contexte numérique global » (p. 212). Elle s'inscrit dans le cadre plus large de la stratégie de sécurité globale de l'entreprise, aux côtés de la sûreté industrielle, des produits et des personnes.

Organisation opérationnelle et mesures de protection

L'entreprise dispose d'une politique de sécurité couvrant « l'ensemble des sites, filiales et employés, y compris les sous-traitants et visiteurs » (p. 212). Cette politique repose sur quatre domaines de sécurité : digitale, industrielle, produits & services, et personnes & environnement de travail. La responsabilité globale revient au Head of Corporate Security, appuyé par le Corporate Security Council et la Digital Security Team.

Les mesures techniques et organisationnelles s'appuient sur des standards reconnus comme ISO 27001. Airbus met en œuvre des « contrôles techniques mesurés selon les standards de gestion de la sécurité de l'information », incluant la protection des terminaux, la prévention des pertes de données, l'authentification multifactorielle et une architecture de sécurité d'entreprise (p. 212).

Pour la détection et la réponse aux incidents, le groupe exploite « des centres d'opérations de sécurité internes (SOC) couvrant les activités commerciales et nationales, ainsi qu'une équipe CERT dédiée ». Ces structures assurent la surveillance en continu et la gestion rapide des incidents.

L'entreprise a également mis en place l'International Security Operating Model (ISOM), un cadre de gouvernance global qui « fournit des orientations et un soutien complet sur les questions de sécurité à toutes les entités internationales et régionales du groupe », avec une mise en œuvre complète prévue en 2025 (p. 212).

Enfin, Airbus investit dans la formation continue à travers son Cybersecurity Diploma and Master's programmes, certifiés par le Registre national des certifications professionnelles français, formant chaque année plusieurs dizaines d'étudiants et collaborateurs (p. 213).

Suivi, audit et indicateurs

Airbus applique un cadre d'audit rigoureux, combinant contrôles internes, évaluations de maturité et audits externes. Le rapport précise que « le système de management de la sécurité est aligné sur la norme ISO 27001, et sa mise en œuvre est suivie à travers divers audits internes et externes » (p. 211). Les principes des trois lignes de défense sont appliqués, avec des Process Review Meetings mensuels assurant le suivi des performances et de la conformité.

En matière d'indicateurs, Airbus affiche une transparence notable : « aucun incident de fuite de données n'a été signalé aux autorités de régulation en 2024 », information validée par l'ANSSI (p. 213). Le Security Operation Centre et le CERT sont responsables de la collecte et de la transmission de ces données. Les Top Functional Objectives de cybersécurité sont fixés chaque année, bien que non publiés pour des raisons de sécurité.

Cette approche intégrée au système global de Enterprise Risk Management (ERM) d'Airbus- basé sur la norme ISO 31000- permet une remontée régulière des risques cyber à la direction et au conseil d'administration (p. 75).

Alignement ESRS 2- GOV / RSK / IRO / SBM (et DC-M / DC-T)

Gouvernance (ESRS 2 GOV-1/2). L'*Annual Report 2024* décrit les rôles du Conseil, des comités et du management en matière de sécurité et de contrôle interne, avec une supervision explicite de la cybersécurité. Cela couvre l'organisation, les responsabilités et les mécanismes de pilotage attendus par ESRS 2.

Risques (ESRS 2 RSK-1). Le dispositif *Risk Management Internal Controls* formalise l'identification, l'évaluation et la mitigation des risques cyber (IT/OT, produits, supply chain). Les processus et contrôles décrits renseignent les exigences RSK-1 (méthodes, périmètre, fréquence des revues).

Matérialité et stratégie (ESRS 2 IRO-1/2 et SBM-3). Les systèmes critiques, la chaîne d'approvisionnement et la transformation digitale ancrent la matérialité cyber. Le rapport relie impacts/risques/opportunités (IRO) à la stratégie et au modèle d'affaires (SBM), en

explicitant les dépendances et les priorités d'investissement.

Indicateurs publiables (DC-M / DC-T). Jeux de mesures typiques pour l'information comparable : *incidents significatifs* (et critères de matérialité), *tests de résilience* (table-top, red-team, exercices de crise), *délais de reprise* (RTO/RPO), *taux de formation/sensibilisation* et *couverture des contrôles clés*. Ces métriques s'alignent avec les rubriques GOV/RSK/IRO et étayent SBM.

Notes : ESRS 2 = exigences générales (GOV : gouvernance, RSK : risques, IRO : impacts / risques / opportunités, SBM : modèle d'affaires / stratégie). DC-M / DC-T = divulgations « Metrics » / « Targets/Tests » mobilisées pour rendre l'information mesurable et comparable.

En conclusion, Airbus démontre une gouvernance cyber mature, soutenue par des processus structurés, des comités dédiés et une intégration transversale dans toutes ses divisions. La stratégie triennale, la conformité aux standards ISO et la coopération entre divisions positionnent l'entreprise parmi les acteurs les plus avancés de son secteur.

Cependant, malgré cette maturité, le rapport reste principalement orienté sur la gestion interne du risque plutôt que sur un reporting détaillé ou audité selon les critères de la CSRD. Les indicateurs publiés demeurent limités, ce qui souligne l'intérêt d'un futur cadre européen plus explicite et contraignant en matière de reporting cybersécurité.

4.2.3 BNP Paribas

BNP Paribas est l'un des principaux groupes bancaires européens, présent dans plus de 70 pays. En tant qu'acteur financier, il gère des volumes considérables de données sensibles et dépend d'infrastructures numériques critiques. Son exposition au risque cyber est donc parmi les plus élevées du secteur tertiaire [5].

Gouvernance et stratégie

BNP Paribas considère la cybersécurité comme un pilier de sa gouvernance des risques et de sa stratégie ESG. Le rapport souligne que « le Groupe investit dans des projets et infrastructures pour sécuriser ses services et soutenir ses clients face aux enjeux numériques »

(p. 81). La supervision est assurée par le Comité exécutif et le Conseil d'administration, qui définissent les orientations en matière de sécurité numérique et de résilience opérationnelle. Le Chief Information Security Officer (CISO) coordonne la stratégie cyber du groupe, en lien avec la direction des risques et la direction de la conformité.

La cybersécurité est également intégrée dans le dispositif global de gestion des risques opérationnels, avec une attention particulière portée aux nouvelles technologies (paiements digitaux, intelligence artificielle, cloud). Le rapport mentionne que ces enjeux « sont au cœur du modèle de développement responsable de la banque » et qu'ils participent directement à la confiance des parties prenantes (p. 31).

Organisation opérationnelle et mesures de protection

Sur le plan opérationnel, BNP Paribas dispose d'une organisation cyber étendue, pilotée par la Direction de la sécurité des systèmes d'information (DSSI). Celle-ci coordonne les équipes locales dans chaque entité et gère plusieurs centres d'opérations de sécurité (SOC) à travers le monde. Le rapport indique que le Groupe met en œuvre des dispositifs de prévention, détection et réaction aux cyberattaques, appuyés sur des technologies d'intelligence artificielle et de machine learning pour l'analyse comportementale (p. 25).

BNP Paribas applique une politique de défense en profondeur, comprenant le chiffrement des données, l'authentification forte, la surveillance des accès privilégiés et la segmentation des réseaux critiques. Une part importante des efforts est consacrée à la formation et à la sensibilisation : chaque collaborateur suit un module annuel obligatoire de cybersécurité, complété par des campagnes de simulation de phishing. Le rapport rappelle que « la vigilance humaine reste la première ligne de défense » (p. 25).

Suivi, audit et indicateurs

Le dispositif de suivi repose sur un contrôle permanent, des audits internes et des évaluations externes. Le rapport précise que « des audits réguliers permettent de renforcer la résilience du Groupe face aux menaces cyber » (p. 25). BNP Paribas suit plusieurs indicateurs internes : taux de conformité aux standards ISO 27001 et NIST, nombre d'in-

cidents détectés, temps moyen de réponse et taux de participation des collaborateurs aux formations.

Les résultats sont consolidés au niveau du Comité des risques, puis présentés au Comité d'audit du Conseil d'administration. Le Groupe collabore aussi avec les autorités de régulation (ACPR, BCE, CNIL) pour s'assurer de la conformité à la directive NIS 2 et aux exigences européennes de résilience opérationnelle (DORA). Ce suivi témoigne d'un haut niveau de formalisation, même si les données publiées restent globales et non détaillées.

Alignement ESRS 2- GOV / RSK / IRO / SBM (et DORA : DC-M / DC-T)

Gouvernance (ESRS 2 GOV-1/2/5). Le *Document d'enregistrement universel 2024 – Corporate Governance and Internal Control* décrit les rôles du Conseil et du contrôle interne, incluant la supervision de la cybersécurité et de la sécurité des SI. Cela couvre les attentes de gouvernance d'ESRS 2.

Risques (ESRS 2 RSK-1). Le cadre *DORA* (Digital Operational Resilience Act) structure l'identification, la classification et la gestion des incidents TIC (technologies de l'information et de la communication). Ces éléments répondent aux exigences de description des risques d'ESRS 2.

Matérialité et stratégie (ESRS 2 IRO-1/2 et SBM-3). La double matérialité et l'intégration de la cybersécurité dans la stratégie sont explicitées : périmètre, impacts, risques / opportunités, liens avec la création de valeur.

Indicateurs publiables (DORA- DC-M / DC-T). Exemples de métriques mobilisables et traçables : – *Incidents TIC majeurs* et *délais de notification* ; – *Couverture des tests de résilience* (TLPT : threat-led penetration testing) ; – *Taux de remédiation des vulnérabilités critiques* ; – *Exigences et résultats de contrôle des tiers critiques*. Ces indicateurs se rattachent aux rubriques **GOV/RSK/IRO** d'ESRS 2 et consolident la section **SBM** (modèle d'affaires et stratégie).

Notes : ESRS 2 = exigences générales de reporting (GOV : gouvernance, RSK : risques, IRO : impacts /risques /opportunités, SBM : modèle d'affaires /stratégie). DORA = résilience

opérationnelle numérique ; DC/M et DC/T désignent les « mesures » et « tests » opérationnels mobilisables pour des KPI.

En conclusion, BNP Paribas présente une gouvernance cyber solide, soutenue par des structures dédiées, des investissements constants et une intégration claire dans la gestion globale des risques. La cybersécurité est perçue comme un facteur essentiel de résilience et de confiance. Toutefois, le reporting reste majoritairement qualitatif : peu d'indicateurs chiffrés sont publiés, et les performances cyber ne sont pas encore intégrées de façon explicite dans le reporting ESG selon la logique de la CSRD. Le Groupe se distingue néanmoins par la maturité de son dispositif, son alignement sur les standards internationaux et son approche équilibrée entre gouvernance, technologie et culture de sécurité.

4.3 Synthèse comparative

Le tableau comparatif ci-après synthétise, pour trois grands groupes (TotalEnergies, Airbus, BNP Paribas), la place de la cybersécurité dans la **gouvernance et l'intégration stratégique**, les **capacités opérationnelles et mesures de protection**, ainsi que le **suivi, l'audit et les indicateurs** publiés. Il offre une lecture rapide du niveau de maturité et des points forts de chaque acteur, tout en révélant une limite récurrente : malgré des dispositifs souvent avancés, le **reporting public** demeure hétérogène et peu chiffré, ce qui complique la **comparaison objective** entre entreprises.

Entreprise	Gouvernance et intégration stratégique	Maturité opérationnelle et mesures de protection	Reporting et transparence	Conformité aux standards / certifications	Remarques
TotalEnergies	Comité Exécutif supervise les risques cyber. La cybersécurité est intégrée à la stratégie globale ESG.	Équipe dédiée, dispositifs IDS et chiffrement, formation régulière.	Reporting encore général, peu d'indicateurs chiffrés.	ISO 27001, NIST	Approche structurée, mais manque de métriques pour comparabilité.
Airbus	Gouvernance centralisée, Comité Exécutif impliqué, cybersécurité intégrée aux projets stratégiques (IA, défense, énergie durable).	Corporate Technical Office pour IT, produits et systèmes industriels. IDS et chiffrement déployés.	Reporting qualitatif détaillant les initiatives stratégiques. Peu d'indicateurs chiffrés.	ISO 27001	Proactive, intégrée à la stratégie, mais indicateurs quantitatifs limités.
Siemens	Gouvernance centralisée, pilotée au Comité Exécutif. Participation à Charter of Trust.	Équipe dédiée pour IT et OT. Protection avancée : IDS, pare-feu, chiffrement.	Reporting détaillé, inclut nombre d'incidents et conformité aux standards.	ISO 27001:2022	Reporting le plus complet parmi les 5, avec indicateurs quantitatifs.

FIGURE 2 – Synthèse de la place de la cybersécurité dans le reporting de trois grandes entreprises

4.4 Conclusion de l'étude de cas

Les trois acteurs ancrent la cybersécurité au plus haut niveau (Conseil/Comex/CISO) et disposent de moyens techniques et organisationnels conséquents (SOC/CERT, formation, politiques, audits). En revanche, leur reporting public reste majoritairement qualitatif et hétérogène : peu publient un noyau de KPI cyber réellement comparables (ex. incidents significatifs, délais de détection/réponse, couverture de formation, résilience IT/OT). Il n'existe pas à ce stade de base claire et standardisée de reporting cyber applicable à tous ; cette lacune rend les comparaisons objectives et transversales difficiles, malgré des dispositifs internes souvent matures. Un socle minimal d'indicateurs audités, harmonisé dans l'esprit CSRD/ESRS, améliorerait nettement la lisibilité et la comparabilité entre entreprises.

En conclusion, il n'existe pas encore de base claire et homogène de reporting de la cybersécurité : chaque entreprise décrit sa gouvernance et ses moyens, mais les indicateurs publiés restent parcellaires, hétérogènes et souvent qualitatifs. Faute d'un noyau commun de KPI audités (ex. délais de détection/réponse, incidents significatifs, couverture de formation, résilience IT/OT), il demeure difficile de comparer objectivement les situations et les niveaux de maturité cyber d'un acteur à l'autre, même quand les dispositifs internes sont robustes. Un cadre européen plus explicite (dans l'esprit CSRD/ESRS) avec quelques exigences minimales de métriques améliorerait nettement la lisibilité et la comparabilité des informations.

5 Conclusion

Au moment où l'Union européenne redéfinit les obligations de transparence extra-financière par la CSRD, un paradoxe majeur émerge. Les cyberattaques augmentent en fréquence et en gravité, affectant tant les infrastructures critiques que les opérations ordinaires. Pourtant, la cybersécurité demeure insuffisamment intégrée dans le reporting de durabilité.

Ce mémoire s'est proposé d'explorer ce décalage et de proposer des voies pour y remédier. En examinant les fondements théoriques et réglementaires (section 2), l'état des standards internationaux (section 3), et la réalité des pratiques du secteur privé (section 4), cette recherche a cherché à répondre à une question centrale : comment intégrer la cybersécurité comme facteur de matérialité dans la CSRD ?

Les analyses suivantes synthétisent les principaux enseignements. Elles identifient les limites de l'étude et dégagent les perspectives pour un cadre régulateur plus robuste et harmonisé.

5.1 Réponse à la problématique et principaux enseignements

Cette thèse explore comment intégrer la cybersécurité en tant que facteur de matérialité dans le cadre de la CSRD. L'analyse menée révèle que si la réponse est affirmative sur le plan théorique, sa mise en œuvre opérationnelle reste inachevée.

Sur le plan conceptuel, le cadre de la CSRD offre une base solide. Le principe de double matérialité justifie l'intégration systématique de la cybersécurité. Comme l'a montré la section 2, la cybersécurité affecte directement les trois piliers ESG.

Elle contribue à la réduction de l'empreinte carbone numérique (dimension environnementale). Elle protège les droits des individus et la confidentialité des données (dimension sociale). Elle préserve les actifs numériques et la résilience financière (dimension économique et gouvernance).

Ces liens multiples justifient une reconnaissance de la cybersécurité comme un enjeu matériel à part entière. Elle devrait être comparable aux risques climatiques ou sociaux.

Sur le plan réglementaire, l'analyse comparative des standards (section 3) révèle une absence criante. Il n'existe pas de cadre européen contraignant, clair et transversal dédié à la cybersécurité. Des référentiels comme ISO 27001, NIST CSF, NIS2, RGPD et DORA apportent des contributions importantes. Cependant, aucun ne combine les dimensions techniques, stratégiques et de reporting de manière systématique.

Les ESRS actuels (ESRS 1 et 2) mentionnent la cybersécurité de manière implicite. Ils le font via la gouvernance et la gestion des risques. Mais ils manquent d'exigences explicites, mesurables ou comparables. Cette lacune contraste avec l'importance croissante des cyberattaques. Les incidents belges récents l'illustrent bien : Brussels Airport (septembre 2025) et Service public de Wallonie (avril 2025).

Sur le terrain, l'étude de cas (section 4) confirme ce diagnostic. Les trois grandes entreprises analysées disposent de gouvernances cyber sophistiquées. TotalEnergies, Airbus et BNP Paribas possèdent chacun un CISO, un SOC/CERT, des audits externes et des stratégies dédiées. Leur maturité interne est indéniable.

Cependant, leur reporting public demeure hétérogène et majoritairement qualitatif. Aucune n'expose un noyau commun et audité de KPI cyber. Les délais de détection/réponse ne sont pas standardisés. Les incidents significatifs ne sont pas définis uniformément. La couverture de formation varie. La résilience IT/OT n'est pas mesurée de la même manière.
Cette absence d'harmonisation rend les comparaisons objectives impossibles. C'est un paradoxe : les meilleures pratiques existent, mais restent invisibles aux investisseurs et parties prenantes.

5.2 Limites de l'étude

Cette recherche présente plusieurs limites à reconnaître.
Sur le plan méthodologique, l'étude de cas repose sur un échantillon limité. Trois entreprises seulement, trois secteurs différents. La période d'observation est restreinte (rapports 2024). Les conclusions révèlent des tendances, mais ne prétendent pas à l'exhaustivité. Un échantillon plus large aurait renforcé la robustesse. Une analyse sur plusieurs années aurait apporté plus de profondeur.
Sur le plan **temporel**, cette thèse est rédigée dans un contexte de transition. Les normes sectorielles ESRS ne seront finalisées qu'en juin 2026. Le paysage réglementaire européen continue d'évoluer. La transposition de NIS2 progresse. L'impact de DORA s'étend. Les conclusions devront être réévaluées à mesure que le cadre se stabilisera.
Sur le plan du **périmètre**, cette étude se limite à l'Europe. Elle couvre seulement les grandes entreprises cotées. Elle n'explore pas les PME. Elle ne traite pas les variations liées aux transpositions nationales. Ces éléments peuvent introduire des nuances importantes selon les États membres.

5.3 Perspectives et recommandations pour l'avenir

Malgré ces limites, cette recherche débouche sur plusieurs perspectives concrètes.
À court terme, l'EFRAG doit renforcer les normes sectorielles ESRS. Il faut inclure des exigences explicites de reporting cyber. La gouvernance des incidents doit être clarifiée. Les indicateurs de résilience IT/OT doivent être définis. La conformité à ISO 27001 et NIST doit être mesurable. La couverture de formation doit être quantifiée.
Un corpus minimal d'indicateurs auditables améliorerait la lisibilité. Harmonisé dans l'esprit

CSRD, il renforcerait la comparabilité entre entreprises.

À moyen terme, une articulation plus claire s'impose. Il faut lier la CSRD/ESRS aux régimes existants : NIS2, DORA, RGPD. Plutôt que de créer un nouveau standard, il s'agit de consolider. Il faut standardiser le reporting public sur la base de cadres existants. Cela évite les redondances. Cela renforce la traçabilité.

À long terme, la cybersécurité mérite une place autonome. Elle doit figurer dans la matrice de double matérialité comme thème stratégique. Elle sera comparable au climat ou à la biodiversité. Cela signifie améliorer les lignes directrices. Cela veut dire valoriser les bonnes pratiques observées chez les pionniers. TotalEnergies et Airbus sont des modèles. Leurs pratiques doivent devenir base de normalisation.

5.4 Conclusion générale

En réponse à la question centrale, oui, la cybersécurité doit être intégrée comme facteur de matérialité dans la CSRD. Les arguments théoriques sont solides. Les risques sont réels. Les précédents réglementaires montrent la voie : SEC, DORA, NIS2.

Cependant, cette intégration ne peut réussir que sous certaines conditions. Il faut un cadre européen contraignant. Il doit être clair et transversal. Il doit associer exigences de gouvernance, indicateurs auditables et comparabilité entre entreprises.

La route vers une cybersécurité véritablement durable ne fait que commencer. La durabilité signifie résilience, transparence et responsabilité. Les défis numériques à venir demanderont une mobilisation collective. Les régulateurs, entreprises, investisseurs et société civile doivent s'engager.

Cette thèse espère y avoir apporté une contribution. Elle cartographie les lacunes. Elle propose un chemin pragmatique vers l'intégration de la cybersécurité dans le reporting de durabilité européen.

Références

[1] Belga News Agency. Cyberattack causes disruption at brussels airport, 2025.

[2] Airbus. Our worldwide presence, 2025.

[3] Airbus SE. Rapport annuel 2024, 2024.

[4] Aviation24.be. Brussels airport to accelerate rollout of new check-in system after cyberattack on collins aerospace software, 2025.

[5] BNP Paribas. Bnp paribas worldwide, 2025.

[6] BNP Paribas. Document d'enregistrement universel et rappor financier annuel 2024, 2025.

[7] BNP Paribas. Rapport intégré 2024, 2025.

[8] Commission européenne. Questions and answers : Corporate sustainability reporting directive (csrd). https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4043, 2023.

[9] Commission européenne. Esrs g1 – conduite des affaires, 2025.

[10] Commission européenne. Esrs s1 — personnel de l'entreprise, 2025.

[11] Adrien DEFER. Generating realistic background traffic using ghosts framework, 2023.

[12] DXC Technology. Environmental, social and governance (esg) sasb index fy 2024, 2024.

[13] EFRAG. Esrs set 1 – 2023 final standards. https://xbrl.efrag.org/e-esrs/esrs-set1-2023.html, 2023.

[14] EFRAG. About us – european financial reporting advisory group. https://www.efrag.org/en/about-us, 2025.

[15] ESSEC Solutions Entreprises. Les enjeux actuels de la cybersécurité pour les entreprises. https://essecsolutionsentreprises.com/wp-content/uploads/2022/11/Rapport-Cybers%C3%A9curit%C3%A9-ESSEC-Solutions-Entreprises-1.pdf, November 2022. Rapport de 2022, ESSEC Solutions Entreprises, cabinet de conseil étudiant.

[16] European Union Agency for Network and Information Security (ENISA). Cybersecurity definition and its scope : Definition gaps. https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf, December 2015.

[17] Parlement européen et Conseil de l'Union européenne. Directive 2014/95/UE du Parlement européen et du Conseil du 22 octobre 2014 modifiant la directive 2013/34/UE en ce qui concerne la publication d'informations non financières et d'informations relatives à la diversité par certaines grandes entreprises et certains groupes. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014L0095, Octobre 2014.

[18] Parlement européen et Conseil de l'Union européenne. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données). https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679, Avril 2016.

[19] Parlement européen et Conseil de l'Union européenne. Directive (UE) 2022/2464 du Parlement européen et du Conseil du 14 décembre 2022 modifiant le règlement (UE) n° 537/2014, la directive 2004/109/CE, la directive 2006/43/CE et la directive 2013/34/UE en ce qui concerne la publication d'informations en matière de durabilité par les entreprises. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2464, Décembre 2022.

[20] Parlement européen et Conseil de l'Union européenne. Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2554, Décembre 2022.

[21] Commission européenne. Finance durable : plan d'action de la commission pour une économie plus verte et plus propre. https://ec.europa.eu/commission/presscorner/api/files/document/print/fr/ip_18_1404/IP_18_1404_FR.pdf, 2018.

[22] Commission européenne. Document de travail des services de la commission – résumé de l'analyse d'impact accompagnant la proposition de directive du parlement européen et du conseil modifiant la directive 2013/34/ue en ce qui concerne la publication d'informations en matière de durabilité par les entreprises. https://eur-lex.europa.eu/legal-con

tent/FR/TXT/PDF/?uri=CELEX:52021SC0151, 2021.

[23] Commission Européenne. Proposition de directive du Parlement européen et du Conseil modifiant la directive 2013/34/UE en ce qui concerne la publication d'informations en matière de durabilité par les entreprises (Directive CSRD). https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52021PC0189, Avril 2021.

[24] Commission Européenne. Règlement délégué (UE) 2023/2772 de la Commission du 31 juillet 2023 complétant la directive 2013/34/UE du Parlement européen et du Conseil en ce qui concerne les normes d'information en matière de durabilité. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02023R2772-20231222, Juillet 2023.

[25] Commission Européenne. European Green Deal – Priorities 2019–2024. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en, 2024.

[26] GIP ACYMA. Cybermoi/s 2024 : un mois pour tous devenir #CyberEngagés. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/2024-cybermois, 2024. Plateforme nationale d'assistance aux victimes de cybermalveillance.

[27] GIP ACYMA. Rapport d'activité 2024. https://www.cybermalveillance.gouv.fr/medias/2025/03/250403_RA_2024_SCREEN.pdf, mars 2024.

[28] Global Reporting Initiative. Gri 418 : Customer privacy 2016, 2016.

[29] Global Reporting Initiative. Digitalization impacts – identifying emerging reporting challenges and needs, 2024.

[30] Corentin HERICHER. Responsabilité sociétale de l'entreprise. Jeu de diapositives universitaire, 2025.

[31] IAS Plus. Le parlement européen approuve le report de certains esrs, 2024.

[32] International Organization for Standardization (ISO). Iso/iec 27001 :2022 — systèmes de management de la sécurité de l'information — exigences, 2022.

[33] International Telecommunication Union (ITU). Itu official website. https://www.itu.int/en/Pages/default.aspx, 2025. Consulté en juillet 2025.

[34] ISACA. Cobit® 2019 framework : Introduction and methodology, 2018.

[35] KPMG. Cybersecurity in esg, 2023.

[36] KPMG. La sec finalise les règles de cybersécurité, 2024.

[37] Ministère de la Transition Écologique. Responsabilité sociétale des entreprises (rse). https://www.ecologie.gouv.fr/politiques-publiques/responsabilite-societale-entreprises, 2024. Consulté en juillet 2025.

[38] MSCI Inc. Msci esg ratings methodology : Privacy & data security key issue, March 2024.

[39] National Institute of Standards and Technology (NIST). The nist cybersecurity framework (csf) 2.0, February 2024.

[40] National Institute of Standards and Technology (NIST). Cybersecurity Framework 2.0 (CSF 2.0). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, Février 2024.

[41] National Institute of Standards and Technology (NIST). Cybersecurity Framework FAQs. https://www.nist.gov/cyberframework/faqs, 2024.

[42] Parlement européen et Conseil de l'Union européenne. Directive (ue) 2022/2555 du parlement européen et du conseil du 14 décembre 2022 concernant des mesures visant à garantir un niveau élevé commun de cybersécurité dans l'union, modifiant le règlement (ue) n° 910/2014 et la directive (ue) 2018/1972, et abrogeant la directive (ue) 2016/1148, 2022.

[43] Nadja Picard, Cécile Saint-Martin, Kevin O'Connell, and Lynne Baber. In search of sustainable value : The csrd journey begins — first reporters study, 2025.

[44] Portail RSE - République Française. Double matérialité : l'analyse des impacts, risques et opportunités. https://portail-rse.beta.gouv.fr/csrd/double-materialite-comprendre-et-appliquer-cette-analyse-essentielle-pour-le-reporting-de-durabilite/, Octobre 2024.

[45] Service public de Wallonie. Détection d'une intrusion d'ampleur dans le système informatique du service public de wallonie, 2025.

[46] PwC France. Directive nis 2 : un nouveau cadre pour renforcer la cybersécurité et la résilience à l'échelle de l'union européenne, 2025.

[47] Securities and Exchange Commission. Cybersecurity risk management, strategy, governance, and incident disclosure, July 2023.

[48] Securities and Exchange Commission. Mission, 2023.

[49] Sustainability Accounting Standards Board (SASB). À propos de sasb, 2025.

[50] Sustainalytics. Esg risk ratings – material esg issue : Data privacy and security, January 2022.

[51] TotalEnergies. Totalenergies dans le monde, 2025.

[52] TotalEnergies SE. Document d'enregistrement universel 2024, March 2025.

[53] Wikipedia contributors. Global reporting initiative, 2025.