Cigref
RÉUSSIR
LE NUMÉRIQUE

Gouvernance de la sécurité numérique

Orientation, déploiement et pilotage

Mars 2026

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Cigref

En partenariat avec l'ANSSI

Gouvernance de la sécurité numérique

Orientation, déploiement et pilotage

Mars 2026

ÉDITO

Depuis maintenant quelques années, la grammaire de la sécurité numérique ne se conjugue plus au conditionnel et la question n'est plus tant de savoir *si* une organisation sera ciblée, ni même *quand*, mais *combien de fois* elle devra faire face à une menace cyber.

En 2025, la menace cyber se stabilise à un niveau particulièrement élevé et s'inscrit dans un contexte d'aggravation des tensions géopolitiques mondiales. La pression exercée sur les entreprises et les services publics reste intense et universelle, avec un partage croissant des moyens et des pratiques des attaquants qui tend à brouiller la frontière entre la menace étatique et cybercriminelle. Cet effet rend l'identification des commanditaires réels de plus en plus complexe, en particulier du fait d'un partage d'outils et de méthodes, ou bien du recours à des infrastructures d'anonymisation. En outre, l'industrialisation et l'hybridation des attaques sont des tendances aussi marquantes pour les années qui viennent, de même que l'effacement des frontières traditionnelles entre l'exfiltration de données, le rançongiciel, la prédation économique, l'espionnage stratégique et le sabotage. Dans ce contexte, face à des attaquants prêts à exploiter chaque faiblesse, tous les acteurs et chaque information comptent en matière de cyberdéfense.

La cybersécurité ne peut donc plus être envisagée seulement comme une fonction technique ; elle devient un élément structurant de la confiance, conditionnant à la fois la sécurité numérique, la résilience et l'autonomie stratégique des organisations. Dès lors, intégrer la cybersécurité au cœur des stratégies numériques implique non seulement des dispositifs techniques adaptés, mais aussi une coordination étroite avec les filières numériques ainsi que l'implication de la gouvernance haute des organisations. Le déploiement des stratégies numériques, en particulier des nouvelles technologies comme l'intelligence artificielle, ne peut se faire sans confiance, et la confiance ne peut s'obtenir sans sécurité. Les comités des risques, comités exécutifs et les conseils d'administration doivent donc être pleinement responsabilisés dans la bonne maîtrise des risques cyber.

Ce rapport réalisé par le Cigref et ses membres, avec le support des équipes de l'ANSSI, est un appel à la prise de conscience, à l'outillage et à la mobilisation collective pour faire de la sécurité numérique un enjeu de gouvernance global, au bon niveau stratégique des organisations.

Vincent Strubel,

Directeur général de l'ANSSI

ÉDITO

L'époque où la sécurité numérique pouvait être perçue comme une simple question d'experts techniques, ou une formalité à respecter pour la conformité, est bel et bien révolue. Dans un contexte marqué par l'instabilité géopolitique et l'hybridation des menaces, la sécurité numérique s'impose comme un pilier fondamental de la pérennité des modèles organisationnels, économiques et même politiques. Le premier message de ce rapport, conçu collégialement au Cigref et co-publié avec l'ANSSI, est de souligner que structurer la gouvernance de la sécurité numérique n'est plus une option. Cette gouvernance constitue désormais pour les organisations un impératif de résilience et, pour ce qui regarde les services et prérogatives étendues de l'État, comme un impératif de souveraineté. L'enseignement principal de ces travaux consiste à proposer des moyens concrets pour structurer une gouvernance robuste autour de trois vecteurs stratégiques : la définition de la politique de sécurité numérique (PSN), son application au quotidien et son pilotage.

Le paysage auquel nous faisons face est en pleine mutation. L'extension continue des surfaces d'exposition, couplée à une industrialisation de la menace, impose une vigilance constante. Face à ces évolutions structurantes, l'anticipation et l'adaptation deviennent des éléments différenciants, pour disposer des capacités non seulement défensives, mais plus proactives de la résilience numérique. La réponse à ces défis n'est pas uniquement technologique, elle est aussi organisationnelle et humaine. Ce rapport a donc eu l'ambition de mettre en lumière la diversité des modèles de gouvernance, adaptés au contexte propre de chaque organisation.

Par ailleurs, si le dialogue doit impérativement monter en puissance au sein des comités exécutifs et des conseils d'administration pour traiter le risque numérique à son juste niveau stratégique et selon les responsabilités respectives, l'enjeu est tout aussi prégnant pour l'ensemble des strates de l'organisation. La culture de la sécurité doit pouvoir infuser suffisamment pour que chaque collaborateur, quelle que soit sa fonction, devienne un acteur éclairé de la protection collective.

Cette exigence de responsabilité partagée s'étend également à l'écosystème au sein duquel chaque organisation s'inscrit. La coopération public-privé doit se renouveler et s'approfondir pour faire face aux nouvelles menaces systémiques. L'ensemble des fournisseurs de l'organisation doit être intégré dans l'analyse de résilience, avec un accent particulier sur les solutions numériques bien sûr, mais pas exclusivement : toute relation fournisseur a désormais un volant numérique, dont la solidité et la résilience doit être appréciée. Enfin, comme gouverner revient à prévoir, la préparation de la crise et la préparation à la crise, quelle qu'en soit l'origine et la nature, doivent pouvoir s'ancrer dans les pratiques quotidiennes des organisations.

Ces travaux d'intelligence collective menés au Cigref, en collaboration étroite avec l'ANSSI dont nous remercions l'implication majeure et les contributions expertes, proposent des repères concrets et des archétypes de gouvernance, pour donner les clés d'une démarche lucide aux décideurs numériques et dirigeants. Je vous souhaite une lecture inspirante pour définir vos futures orientations stratégiques, et contribuer ainsi au renforcement de la résilience numérique de nos organisations, et donc de notre société.

Mathieu Weill,

Secrétaire général adjoint chargé du numérique au ministère de l'Intérieur

RÉSUMÉ EXÉCUTIF

1. Structuration de la gouvernance de la sécurité numérique comme nouvel impératif stratégique

La sécurité numérique s'est affranchie de son statut de sous-jacent technologique pour s'imposer comme une condition de la pérennité, de la performance et de la compétitivité des organisations. Face à une menace hybride, industrialisée et d'une haute intensité persistante, le risque de sécurité numérique se maintient au premier rang de ceux qui pèsent sur la résilience des organisations.

Ce changement de paradigme, particulièrement manifeste dans un contexte géopolitique en pleine recomposition, est entériné depuis octobre 2024 par la directive européenne NIS2, qui élève la sécurité numérique au rang d'enjeu stratégique majeur pour de nombreuses organisations. La responsabilité légale des mandataires sociaux y est désormais directement engagée en matière d'approbation du cadre de gouvernance et de contrôle des stratégies de sécurisation. La structuration d'une gouvernance dédiée ne peut plus être considérée comme une option de « bonne gestion » et doit s'affirmer comme une « exigence vitale » nécessitant l'implication continue de toutes les strates de l'organisation, à commencer par celle des instances décisionnelles.

2. Trois vecteurs d'une gouvernance de la sécurité numérique au service de la résilience

Pour faciliter la lisibilité de l'action à mener et la bonne répartition des tâches, la réflexion collégiale des membres du groupe de travail Cigref a structuré la gouvernance autour des 3 vecteurs.

Le premier vecteur réside dans la construction et l'endossement de la Politique de Sécurité Numérique (PSN). Dépassant le seul périmètre de la sécurité du système d'information (PSSI), la PSN fait de la sécurité numérique un levier de résilience global, notamment face aux conséquences géopolitiques, juridiques et économiques des dépendances technologiques. Cette politique se matérialise par une feuille de route pluriannuelle qui aligne cartographie et seuil d'acception des risques, qui oriente l'allocation des ressources proportionnées à la criticité des actifs, qui garantit l'autonomie stratégique de l'organisation face à son écosystème et qui prévoit le transfert assurantiel des risques résiduels.

Le deuxième vecteur s'articule autour de la mise en application, au quotidien, de la PSN. L'objectif principal est d'assurer en continu les capacités de résilience (préventives et proactives) par la structuration des équipes et la sécurité de l'ensemble du cycle de vie des actifs. L'acculturation globale aux bonnes pratiques « d'hygiène numérique », le dialogue et les entraînements réguliers entre la fonction numérique et les instances décisionnelles représentent des avantages concurrentiels réels.

Le troisième vecteur porte sur le pilotage par les métriques et leur communication ciblée. Ce pilotage impose d'adapter la mesure aux instances de gouvernance : le niveau stratégique requiert des indicateurs de synthèse sur la couverture des risques majeurs ; le niveau décisionnel évalue le retour sur investissement des défenses et la résorption de la « dette de sécurité » ; tandis que le niveau opérationnel surveille la vélocité de remédiation face aux alertes.

3. Matrice des responsabilités des CA et des Comex pour aligner les orientations stratégiques

Pour répondre à la nouvelle donne contextuelle et réglementaire, le rapport des membres du Cigref propose une synthèse de la répartition des responsabilités des instances décisionnelles.

Le conseil d'administration, garant de la pérennité de l'organisation, se positionne comme l'instance qui oriente, associe les parties prenantes et exige une remontée d'information fiable. Il lui revient de fixer formellement l'appétence au risque, de valider la stratégie globale, d'arbitrer les allocations de ressources critiques et d'interroger la direction générale sur la réalité de l'exposition.

Le comité exécutif assume un rôle de proposition, de cadrage et d'impulsion. Sa responsabilité est d'aligner la vision stratégique du Conseil avec les impératifs métiers. En sa qualité de responsable exécutif, le Comex structure la gouvernance interne, orchestre la résilience en « temps calme » comme en « temps de crise », et veille à faire de la sécurité numérique un levier de création de valeur.

4. Quatre archétypes organisationnels pour une gouvernance sur-mesure

La déclinaison de cette gouvernance exige de comprendre qu'il n'existe pas un seul modèle valable universellement. La sécurité numérique doit faire l'objet d'un choix stratégique, calibré selon l'ADN de l'organisation. Quatre archétypes fonctionnels se dégagent, définis par leur proposition de valeur et leur rattachement hiérarchique privilégié :

- **L'archétype « Expert et partenaire »**, avec une proposition de valeur centrée autour des besoins métiers et de l'innovation technologique, avec une approche de facilitateur d'affaires et de partenaire proactif ;
- **L'archétype « Conformité et affaires publiques »**, avec une proposition de valeur centrée autour de la gestion des risques, avec une approche par la conformité et les affaires publiques dans les processus législatifs et normatifs ;
- **L'archétype « Plateformisation et gouvernance »**, avec une proposition de valeur centrée autour de l'expansion autonome de la sécurité numérique, avec définition et suivi du cadre de gouvernance et partage des responsabilités ;
- **L'archétype « Sécurité intégrée »**, avec une proposition de valeur centrée autour de la gestion du continuum de la menace, avec portage de la responsabilité de la sécurité opérationnelle globale des actifs physiques et numériques.

5. Principes d'actions pour une gouvernance performante et compétitive

Pour consolider ce dispositif, le rapport met en lumière plusieurs grands principes à actionner selon chacun des 3 vecteurs de gouvernance :

Le premier vecteur exige de faire primer le réalisme et la coopération avant toute solution purement technique. Les dirigeants doivent aligner l'effort de sécurité sur les critères essentiels et différenciants de création de valeur, ce qui impose de décloisonner l'organisation pour responsabiliser ses parties prenantes, en interne, et de s'inscrire dans une démarche de défense collective, avec ses tiers.

Le second vecteur requiert d'aligner le dispositif avec l'organisation existante. La gouvernance doit clarifier les mandats, mutualiser certaines compétences et permettre de trancher rapidement les arbitrages vitaux, tout en maintenant une vigilance étendue sur l'écosystème et le facteur humain.

Le troisième vecteur enjoint à privilégier des indicateurs concrets et ciblés. Soigneusement adaptés aux différents niveaux de décision, ces indicateurs doivent permettre de maîtriser la dette technique, d'entretenir la réactivité opérationnelle et de partager les résultats dans un cadre de confiance, dotant ainsi l'organisation d'une véritable vision systémique de sa résilience.

REMERCIEMENTS

Nos remerciements vont à Mathieu Weill, Secrétaire général adjoint chargé du numérique au Ministère de l'Intérieur, qui a piloté nos travaux, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail Cigref (ordre alphabétique) :

Romuald ANGOT - AG2R LA MONDIALE

Youna BARANCIRA - SAUR

Bruno BATISSE - MICHELIN

Paul BÉCU - COVÉA

Laurent BENDAVID - DASSAULT AVIATION

Marie-Sylvie BIZIEN - TESSADRI - SNCF

Aline BOURDIN - VINCI

Marine BROUSSOT - BNP PARIBAS

Hecham CHERIFI - GROUPE BPCE

Claudio CIMELLI - MINISTÈRE DE L'ÉDUCATION

Raffaella CORTELLESI - TRANSDEV GROUP

Mathieu COUTURIER - ANSSI

Jean-Marc DO LIVRAMENTO - ENEDIS

Jean-François DUPITIER - FRANCE TRAVAIL

Freddy ELMALEH - INVIVO

Catherine FITREMANN - GROUPE BPCE

Pascal FLORIN - OSIIC

Karine JOSEPHINE - MINISTÈRE DES ARMÉES

Sergio KAC - ESSILORLUXOTTICA

Stéphane LAPALUT - AIR FRANCE-KLM

Yoann LEGER - FRANCE TRAVAIL

Jérôme LÉGER - CRÉDIT AGRICOLE SA

Ambre LUONG - SERVIER

Gino MEUL - GROUPE AVRIL

MONNERET Michel - MEFSIN

Benjamin MORIN - MINISTÈRE DE L'INTÉRIEUR

Chiraz OUELHAZI - CAISSE DES DÉPÔTS

Marie-Christine PARENT - MEFSIN

Nicolas PERRIN - BANQUE DE FRANCE

Franck POLI - CRÉDIT AGRICOLE SA

Patrick PROSPER - GROUPAMA SUPPORTS & SERVICES (G2S)

Frédéric RIGA - GETLINK

Nacira SALVAN - MINISTÈRE DE L'INTÉRIEUR

Mariana SEGOVIA FERREIRA - FAYAT IT

Olivier SIEGLER - PIERRE FABRE

Vincent TROUILLON - TRANSDEV GROUP

Sébastien VALSEMEY - SOMFY

Sylvie VIALLET - OPMOBILITY

Mathieu WEILL - MINISTÈRE DE L'INTÉRIEUR

Nous remercions également vivement tous les intervenants qui ont nourri la réflexion de notre groupe de travail :

- Michael Barthellemy, OCSSI chez Airbus Commercial
- Jean-François Bobier, Partner & VP Product Management chez BCG Paris Cyber
- Patrick Prosper, DSES - RSSI Groupe chez Groupama
- Olivier Pujol, VP Governance, Risk & Compliance chez Airbus
- Anne Tricot, Chief of Staff at Head of CSO chez Airbus
- Adnène Trojette, Principal chez BCG Paris Cyber
- Frédéric Riga, Chief Digital Officer chez GETLINK
- Vincent Strubel, Directeur général de l'ANSSI

Merci enfin à Gérôme Billois (Partner chez Wavestone), Léa Merveilleau (Consultante chez Wavestone), Franck Poli (Group CISO du Crédit Agricole) et Caroline Ruellan (Présidente du Cercle des Administrateurs), pour leurs points de vue d'experts et retours d'expérience.

Ce document a été construit et rédigé par Pierre Skrzypczak, Chargé de mission senior Stratégie et Prospective au Cigref.

Il vise à formaliser les travaux du groupe de travail « Gouvernance de la sécurité numérique », auquel ont contribué les membres du Cigref au cours des 6 sessions de travail de l'année 2024-2025.

Il restitue donc principalement les acquis, les avancées, les expériences, les défis et les questionnements des représentants des grandes administrations publiques et entreprises privées françaises afin d'en faire bénéficier leurs pairs et l'écosystème numérique au sens large.

Il est prioritairement destiné à nourrir les dialogues avec les comités exécutifs et les conseils d'administration.

TABLE DES MATIÈRES

TABLE DES SYNTHÈSES GRAPHIQUES

TABLE DES RETOURS D'EXPÉRIENCE

INTRODUCTION

CONTEXTE, TENDANCES ET PERSPECTIVES DE LA SÉCURITÉ NUMÉRIQUE

L'omniprésence du numérique dans les sphères professionnelles et institutionnelles s'accompagne d'une expansion continue des risques numériques et par là-même du rôle à jouer par les décideurs du plus haut niveau, en matière de sécurité numérique. Dans un contexte où la question n'est plus de savoir « qui sera la prochaine cible ? », ni même « quand serai-je attaqué ? » mais « combien de fois le serai-je ? », le pilotage par les risques de la sécurité numérique devient un élément aussi essentiel que différenciant.

En matière de sécurité numérique, la menace pour les organisations françaises ne cesse de s'intensifier depuis 2020. **L'Agence nationale de la sécurité des systèmes d'information (ANSSI) constate en 2025** [1] **un niveau de menace qui reste élevé, qui n'épargne personne et qui est le fait d'attaquants toujours plus difficiles à suivre.** La montée en puissance des attaques par déni de service distribué (doublement des DDoS en 2024 par rapport à 2023), à l'instar de celles qui ont eu lieu contre La Poste fin décembre 2025, reflète l'intensification des stratégies de déstabilisation des systèmes critiques, tandis que l'accroissement des attaques ayant un objectif capacitaire renforce la menace de dégradation des actifs opérationnels, en particulier ceux des systèmes industriels.

Les bouleversements du contexte mondial ont des incidences de plus en plus marquées sur la gouvernance globale des organisations. Au plan géopolitique par exemple, les attaques en provenance d'acteurs réputés étatiques ciblant les infrastructures critiques s'intensifient. La porosité croissante entre l'espionnage d'État, le « hacktivisme » et la cybercriminalité constitue également un des faits marquants de l'année 2025. Dans un contexte qui présente de nombreux attributs d'une guerre hybride, les outils et infrastructures sont parfois partagés entre acteurs étatiques et cybercriminels. Ce phénomène brouille les lignes - comme dans les attaques coordonnées sous « faux drapeau » - et permet de détourner des capacités issues de programmes d'espionnage au profit d'usages criminels ou activistes. À cela s'ajoutent les nouvelles offres de lutte informatique offensive (LIO), proposées par des entreprises privées comme l'entreprise israélienne NSO Group, à l'origine du logiciel espion Pegasus. L'augmentation de ces offres privées traduit une banalisation des armes logicielles au-delà du périmètre étatique.

De manière générale, les attaques gagnent en ampleur, en sophistication et en hybridation. Ainsi, l'intelligence artificielle est utilisée pour automatiser et enrichir le ciblage des campagnes d'hameçonnage et de vol d'information par *infostealers* [2]. Cette tendance à l'industrialisation et à la structuration de la menace, qui pourrait s'assimiler à une « offre à la demande » de *Cybercrime-as-a-Service,* cible principalement les chaînes d'approvisionnement matérielles qui sont de plus en plus imbriquées. Les exploitations de vulnérabilités matérielles sont réalisées en amont, notamment sur les divers objets connectés, et en aval, sur les failles logicielles non corrigées. La diversification des risques,

[1] Panorama de la menace, ANSSI, 11 mars 2025

[2] Logiciel malveillant (malware), conçu pour voler de manière discrète des données des appareils qu'il infecte.

par démultiplication croisée des surfaces d'attaques (équipements de bordure, API, cloud-SaaS, *Shadow IT/IA*, convergence IT/OT), des chaînes de valeur étendues (logistique, fournisseurs et tiers en cascade) et des ressources des attaquants, transforme les stratégies de sécurité numérique sur les « trois lignes de maîtrise » (management opérationnel, fonctions support/gestion des risques et audit interne).

Le contexte de la fin d'année 2025 met sous pression les administrations et entreprises privées françaises selon trois modes, qui peuvent dans certains cas se recouper :

- **Premièrement, via le ciblage des fournisseurs de confiance eux-mêmes**, qui sont devenus, comme Microsoft, Fortinet, SolarWinds ou Zscaler, des cibles d'attaques majeures, comme le montre l'exploitation inédite des équipements de bordure (VPN, pare-feu) pour contourner les défenses en profondeur.
- **Deuxièmement, via une sophistication des attaques qui portent sur la chaîne d'approvisionnement logicielle, ou qui exploitent des techniques d'ingénierie sociale** (applications tiers de Salesforce, Sales Loft).
- **Troisièmement, via l'emploi de modes d'attaques plus directs visant des infrastructures considérées par les organisations comme critiques**, à l'image de la récente attaque d'envergure subie par l'opérateur Colt Technology Services, ou encore par le fournisseur de cloud AWS, dont les environnements ont été compromis par exploitation des clés d'accès exposées par TruffleHog.

Les risques associés à la sécurité numérique pèsent au plus haut niveau. Ils sont à la fois :

- **Financiers et réputationnels**, les impacts directs d'une attaque de haute intensité étant évalués en moyenne à 45 millions d'euros (BCG), et pouvant grimper jusqu'à plusieurs milliards d'euros avec des impacts réels sur les PIB nationaux, comme en atteste la cyberattaque contre Jaguar Land Rover.
- **Stratégiques et opérationnels**, les attaques de tiers comme celle d'Harvest en mars 2025 mettant en jeu des données sensibles et ralentissant sectoriellement les activités des organisations bancaires.

Dans ce contexte, il est devenu tout particulièrement important pour les organisations de pouvoir structurer un dispositif résilient de gouvernance de la sécurité numérique qui puisse être à la fois global et transversal, applicable et évolutif, pragmatique et pilotable. Alors que d'éventuelles connexions entre les attaques numériques et les tentatives de déstabilisation de nature étatique, à l'encontre d'institutions et de marques représentatives du bloc occidental, ne peuvent plus être complètement écartées aujourd'hui, le besoin de hisser le niveau de jeu collectif, face à l'état actuel et à venir de la menace, a motivé la création du groupe de travail du Cigref. Ce rapport qui en découle a donc pour objet de proposer un ensemble de moyens visant à faire de la gouvernance de la sécurité numérique un levier de résilience, au service de la performance et de la compétitivité des organisations.

AVIS D'EXPERT

Quels sont les futurs enjeux de la gouvernance de la sécurité numérique à l'horizon 2030 ?

Dans la lignée des gouvernances explicitées dans ce document, la sécurité numérique est appelée à évoluer sous l'effet de transformations profondes des menaces, des technologies et des cadres réglementaires. À l'horizon 2030, plusieurs mouvements, aujourd'hui encore exploratoires, devraient s'imposer et conduire à un élargissement des champs de responsabilité des équipes de sécurité numérique, ainsi qu'à la construction de modes de gouvernance plus transverses, fluides et orientés valeur.

L'évolution des menaces constitue, depuis plusieurs années déjà, un premier facteur structurant. Les menaces dépassent désormais largement le périmètre usuel des organisations et concernent l'ensemble de son écosystème : fournisseurs, prestataires, partenaires, environnements cloud,... Cette extension impose un rapprochement renforcé entre les équipes de sécurité numérique, les achats et les métiers afin d'intégrer le risque cyber dans les relations contractuelles et opérationnelles.

Par ailleurs, les systèmes d'information industriels font face à des menaces spécifiques (pilotage des ouvrages industriels à partir d'outils bureautiques, porosité des architectures SI …) qui nécessitent une coordination étroite avec les directions de la production industrielle ou les DSI lorsque celles-ci en ont la responsabilité.

Enfin, les menaces internes et informationnelles prennent une ampleur nouvelle. La capacité à détecter et analyser des comportements suspects, qu'ils proviennent d'employés, de sous-traitants, de partenaires ou d'agents d'IA, devient de plus en plus essentielle. Elle appelle une gouvernance transversale associant ressources humaines, contrôle interne, lutte contre la fraude et communication, appuyée sur des instances de pilotage permettant des arbitrages éclairés.

Les évolutions technologiques, et en particulier l'essor de l'intelligence artificielle, transforment également les périmètres à gouverner. Les modèles d'IA et les agents autonomes introduisent de nouveaux risques qui dépassent les processus traditionnels de la sécurité des systèmes d'information. Les exigences de « *Responsible AI* », portées notamment par l'*AI Act*, imposent une approche transverse mêlant enjeux juridiques, éthiques, technologiques et de sécurité. Dans ce contexte, la sécurité numérique doit s'inscrire dans une gouvernance globale de l'IA. En miroir, la structuration d'un poste de « *Cyber Data & AI Officer* » au sein des équipes cyber peut permettre d'apporter des réponses opérationnelles, de développer les compétences et d'exploiter l'IA comme levier de résilience et de performance.

D'autre part, la gestion des identités et des accès devient un enjeu central. La multiplication des identités, humaines, techniques ou liées aux agents d'IA, rend nécessaires la simplification et la clarification d'une gestion des identités et des accès (IAM), aujourd'hui souvent trop fragmentée entre métiers, DSI et cybersécurité.

Enfin, le cadre réglementaire continue d'évoluer. Si la gouvernance actuelle permet de répondre efficacement à de nombreux textes existants, de nouvelles exigences émergent, notamment en matière de sécurité des produits numériques. Celles-ci impliquent un rapprochement étroit avec les métiers et pourraient conduire à la création de fonctions dédiées, telles que celle de « *Product Security Officer* », afin d'intégrer la sécurité dès la conception.

L'ensemble de ces évolutions devra être conduit avec une attention constante portée à la création de valeur par la sécurité numérique, en veillant à ce que les dispositifs de gouvernance contribuent non seulement à la maîtrise des risques, mais aussi à la performance, à la confiance et à la résilience des organisations.

Gérôme BILLOIS, Partner Wavestone

Léa MERVEILLEAU, Consultante Wavestone

DÉFINITION ET RAISON D'ÊTRE D'UNE GOUVERNANCE DE LA SÉCURITÉ NUMÉRIQUE

La gouvernance de la sécurité numérique recoupe un ensemble d'activités qui visent à organiser les politiques, procédures et contrôles à mettre en place afin de protéger les activités numériques de son organisation face aux divers risques, menaces et crises.

Elle se déploie notamment sur deux plans :

- **D'une part, elle définit l'articulation entre les actifs et infrastructures, les processus et les responsabilités des différentes parties prenantes**. La valorisation de ce travail de visibilité et de lisibilité des périmètres d'action et des rôles associés peut prendre la forme d'un RACI, garant de la structure de gouvernance.

- **D'autre part, elle orchestre la déclinaison des fonctions de sécurité numérique selon une comitologie à plusieurs niveaux**, avec un *reporting* adapté aux différentes parties prenantes et des réunions de comité échelonnées en fonction des besoins, garants des processus de la gouvernance.

De nombreuses organisations évoluent désormais dans des environnements pluriels et hétérogènes. Cependant, ces environnements ont tous en commun d'être marqués par une volatilité croissante de leurs conjonctures, une ambiguïté persistante dans l'appréciation des situations qu'ils portent et une incertitude croissante pesant sur les capacités de continuité d'activité qu'ils offrent aux organisations. À ces facteurs s'ajoute une complexité systémique due à l'imbrication des chaînes de valeur, internes et externes. Au final, toutes ces dynamiques accroissent de manière profonde et continue la remise en cause des modèles d'affaires et des schémas organisationnels connus et renforcent le besoin d'une stratégie de la sécurité numérique la plus structurée, exhaustive, claire et fluide possible.

La gouvernance de la sécurité numérique n'est pas seulement un enjeu de conformité, elle vise notamment à développer les capacités d'une organisation à anticiper, absorber et surmonter des

perturbations de toute nature qu'elles soient. Elle représente donc un atout de résilience, au service de la compétitivité et de la performance des organisations.

POSITIONNEMENT DE LA GOUVERNANCE, AU CARREFOUR DE MULTIPLES ENJEUX

La gouvernance de la sécurité numérique, à la croisée de différents types de gouvernances, semble à ce jour n'avoir fait que peu l'objet d'études propres. En effet, l'ISACA, dans ses travaux de 2018 sur le sujet, reprend le « modèle des trois lignes » de maîtrise proposé en 2013 par *l'Institute of Internal Auditors* (IIA) [3], principalement sous l'angle de la sécurité de l'information et de la gouvernance [4], et la mise à jour par l'IIA en 2020 de ses travaux structurants reste généraliste.

En outre, son articulation avec les autres formes de gouvernance au sein des organisations apparaît comme une thématique peu traitée jusqu'à présent. En effet, la gouvernance de la sécurité numérique ne se confond ni avec la gouvernance du numérique propre à la seule DSI, ni avec la gouvernance globale de l'entreprise. De plus, elle se distingue de la gouvernance dédiée à la gestion de la conformité, des risques et de la sûreté physique et trouve donc dans chaque organisation un espace propre entre les quatre, voire cinq, formes de gouvernance mentionnées, avec lesquelles elle se doit de composer.

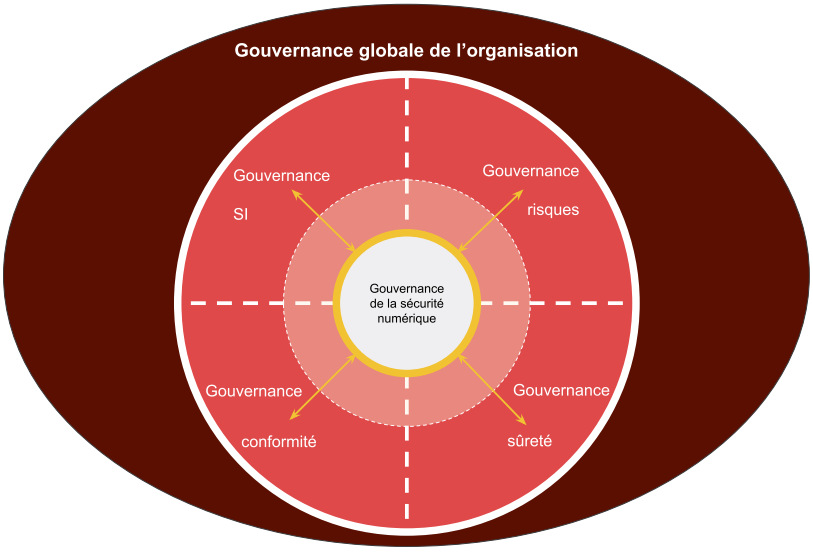


Figure 1 : Positionnement et relations de la gouvernance de la sécurité numérique avec les autres gouvernances au sein des organisations

[3] *The IIA's Three Lines Model - An Update of the Three Lines of Defense*, IIA, 2020
[4] *Rôles des trois lignes de défense pour la sécurité de l'information et la gouvernance*, ISACA, Juillet 2018

ÉVOLUTION ET PROPAGATION DU RISQUE NUMÉRIQUE

La gouvernance de la sécurité numérique des organisations a aujourd'hui une importance toute particulière, dans un contexte de prolifération des menaces et d'élargissement du champ des acteurs ciblés par les attaques cyber.

La menace d'un « Grand soir » ou d'un « Pearl Harbor » cyber qui donnerait lieu à une paralysie généralisée de la société est aujourd'hui bien intégrée dans les échanges internationaux, et des mesures sont prises en faveur de la résilience des organisations et plus globalement, des sociétés. Cependant, force est de constater que loin de peser uniquement sur les États par voie de sabotage, d'espionnage ou de crime organisé, les menaces concernent l'ensemble des acteurs du tissu économique français. Le partage du risque entre l'État et les acteurs nationaux est un prérequis à la prise en compte de cet état de fait, notamment concernant la sécurité de l'espace numérique - véritable pendant de la sécurité physique de l'espace public - et l'assurance face aux dommages causés en la matière.

La prise de conscience et la préparation n'en restent pas moins, bien souvent, insuffisantes face à la montée des menaces dites « systémiques », qui visent tous azimuts et de manière de plus en plus rapide un large panel d'acteurs, procédant par opportunisme et s'attaquant principalement à la réputation des organisations ciblées. Ce nouveau type de menace concerne pourtant tous les acteurs, en raison de l'accroissement technique de la puissance de frappe des attaquants obtenue par automatisation IA. On constate par ailleurs que les attaques actuelles, même provenant d'acteurs cyber criminels très organisés, visent pour bonne part exclusivement le vol des données, et ne vont pas jusqu'au déploiement complet de rançongiciels.

Derrière la faible hausse du nombre total d'incidents se cache en réalité une augmentation significative des volumes de données compromises. Ces attaques massives posent la question de la sécurisation des chaînes de valeur pour les clients et pour leurs tiers mais aussi celle de la normalisation de la gestion du risque dans le cadre des activités commerciales et financières critiques, sujet au cœur de la transposition de la directive européenne NIS 2 en France.

La monétisation d'informations stratégiques est plus large et plus rapide, et les données sont dérobées généralement à faible coût mais en grande quantité, à plusieurs clients différents. Cela se traduit notamment par le déclin relatif des attaques par ransomwares au profit du vol et de la revente de données, et la mise en vente d'*infostealers*, de campagnes d'hameçonnage ou de scripts de *scraping* [5]. Cette approche, industrialisée au point que l'on puisse parler de *Cybercrime-as-a-Service*, est plus discrète, moins complexe techniquement, et moins engageante pénalement.

Le profil des attaquants actuels présente, par ailleurs, une forte dimension informationnelle. Certains cyber activistes jouent même de leur image de pirates identifiés pour déstabiliser uniquement par leur communication, comme dans le cas de l'attaque de la *Cyber Army of Russia Board* qui annonçait, au cours des JO de Paris, avoir détérioré des stations d'épuration.

Face à ces menaces en développement, la gouvernance de la sécurité numérique des organisations doit résolument impliquer les plus hautes instances de management pour tirer parti au mieux des

[5] *Scraping* : technique automatisée de récupération et d'organisation de données contenues dans des sites Web.

« temps froids » et réaliser les investissements préventifs nécessaires. L'objectif principal est de construire et d'entretenir en continu des capacités de gestion de crises, avec une attention particulière portée aux menaces pesant sur le positionnement stratégique de l'organisation et au ciblage de ses actifs, systèmes et processus critiques.

DÉFI POUR LES COMEX ET LES CA, AU-DELÀ D'UNE « AFFAIRE DE TECHNICIENS »

La mise en place et le maintien de la gouvernance de la sécurité numérique ne se restreint pas à des questions techniques réservées aux spécialistes de la sécurité.

- **L'intégration des usages numériques au cœur des métiers exige en effet de bien connaître les infrastructures physiques qu'ils requièrent et d'avoir une confiance adaptée dans les capacités réelles qu'ils offrent**. La gouvernance de la sécurité numérique est, d'une part, plus diffuse, et d'autre part plus intégrée nativement dans les couches numériques essentielles.

- **L'ouverture de la cybersécurité à une démarche globale d'organisation, gérée par les risques, requiert une mise en cohérence de l'appétence au risque général avec les enjeux de sécurité numérique.** L'intégration de la cybersécurité aux risques numériques au sens très large rend la question moins technique, moins cloisonnée et plus intelligible et absorbable par les directions métiers.

- **Les besoins en compétences humaines propres à toute forme de gouvernance favorisent l'expansion des problématiques de sécurité numérique au-delà de la sphère technicienne.** *De facto*, l'effet principal de cette forme de gouvernance, en matière de sécurité numérique, est d'arriver à faire naître, et à orienter, prioriser et entretenir, un état d'esprit alerte et critique en toutes circonstances, en recourant à une compréhension fine des problématiques de conduite de changement, de transversalité, et de résilience psychologique aux diverses formes et intensités de tension.

La criticité, l'ampleur et la durée des effets financiers, stratégiques, communicationnels et opérationnels mis en jeu par l'absence ou la mauvaise gestion de cette gouvernance en font un point d'attention stratégique prioritaire pour les comités exécutifs et les conseils d'administration. La prise en compte de l'importance de la sécurité des systèmes d'information au niveau des instances décisionnaires est un fait acquis et une réalité aujourd'hui bien installée. L'extension du périmètre à sécuriser, des SI vers l'ensemble des enjeux numériques des organisations, appelle cependant à repenser les politiques, structures, schémas, et métriques des organisations. L'objectif est aujourd'hui de pouvoir proposer une gouvernance de la sécurité numérique apte à répondre aux nouvelles responsabilités légales des décideurs et à être un levier opérationnel majeur des plans de transformation numérique et des cartographies des risques.

La gouvernance de la sécurité numérique ainsi comprise doit représenter un atout de résilience au service de la compétitivité et de la performance des organisations, dans les différents contextes qui s'imposent à elles.

- **En temps d'accalmie, ou « temps froid »**, quand cette gouvernance participe à l'anticipation des risques et à l'amélioration de la robustesse de la sécurité numérique ;
- **En temps de crise**, quand elle contribue à l'adaptation et à la reconstruction durable et enrichie des dispositifs de sécurité numérique.

Le levier d'action résiliente offert par la gouvernance de la sécurité est également double s'appuyant sur :

- **Une résilience proactive**, par une capacité interne de gestion des risques et d'agilité organisationnelle qui permet, sans contre-attaquer de manière offensive, de prévoir, préparer et tirer parti des circonstances ;
- **Une résilience défensive,** par la capacité d'absorption, de mitigation et de remédiation face aux événements extérieurs qui permet, sans passivité excessive, de résister, maintenir et rebâtir en faisant un bon usage des incidents.

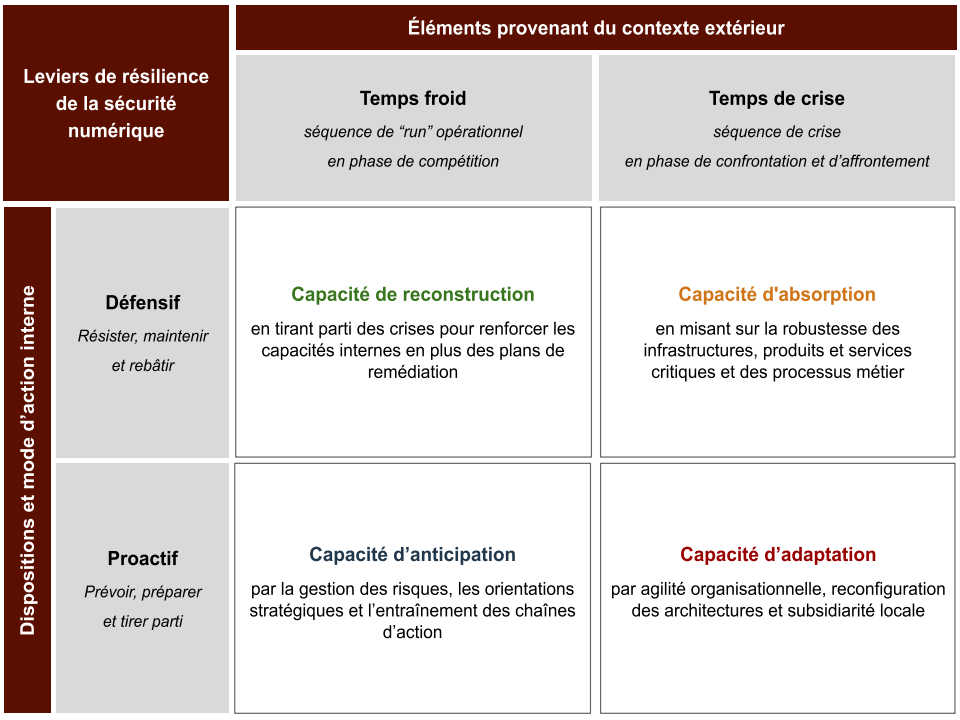


Figure 2 : Les 4 capacités qui structurent la résilience numérique

Fort de ces constats, l'objet principal de ce rapport se portera sur la structuration de la gouvernance de la sécurité numérique et les responsabilités des parties prenantes au plus haut niveau de décision, en nous référant aux différents travaux d'ores et déjà menés au sein du Cigref [6] et de l'ANSSI [7] et aux normes internationales préexistantes [8].

[6] *Anticiper les cyberattaques* (Mars 2024), *Réagir à une cyberattaque massive* (Février 2023), *Auditer la gouvernance du numérique* (Novembre 2023)
[7] *Cartographie du système d'information* (Novembre 2018), *Maîtrise du risque numérique* (Novembre 2019), *La méthode EBIOS Risk Manager* (Juillet 2022), *Anticiper et gérer une crise Cyber* (Juillet 2022), *Cyberattaques et remédiation* (Mars 2024)
[8] *Management du risque* - ISO 31000, *Continuité des activités* - ISO 22301, *Audit de systèmes de management de la sécurité de l'information* - ISO 27001, *Risk Manager* - ISO 27005, *Contrôles de sécurité de l'information* - ISO 27008

1 TROIS VECTEURS DE GOUVERNANCE POUR UNE SÉCURITÉ NUMÉRIQUE AU SERVICE DE LA RÉSILIENCE

Le but de la structuration en trois vecteurs de la gouvernance de la sécurité numérique est de permettre l'optimisation des processus :

- **Aux plans stratégique, organisationnel et opérationnel** ;
- **Au plan des périmètres d'action et des responsabilités** des différentes parties prenantes ;
- **Au plan de la gestion des trois lignes de maîtrise**[9] **proposées par l'IIA,** appliquée à la sécurité numérique de la manière suivante :
  - **Première ligne** portant sur le **management opérationnel**. Elle assure la fourniture des produits et services aux clients et assume la responsabilité première de la gestion des risques au quotidien
  - **Deuxième ligne** portant sur les **fonctions support et la gestion des risques.** Elle apporte une expertise, un soutien, une surveillance, et une remise en question critique sur les sujets liés à la sécurité numérique, pour orienter, superviser et accompagner la première ligne à atteindre ses objectifs.
  - **Troisième ligne** portant sur **l'audit interne.** Elle fournit aux organes de gouvernance une assurance indépendante et objective ainsi que des conseils sur l'adéquation et l'efficacité de la gouvernance et de la gestion des risques, garantissant ainsi une amélioration continue sans être juge et partie.
  - ***Nota Bene* : Une quatrième ligne externe a été ajoutée** à la catégorisation et rassemble les différents fournisseurs, régulateurs et acteurs de l'audit externe. Située hors du périmètre organisationnel *strict*, elle traduit les responsabilités des acteurs intervenant sur la chaîne de valeur étendue, selon qu'ils portent une part du risque opérationnel, ou qu'ils favorisent et objectivent le cadre de conformité, de confiance et de sécurité à l'échelle.

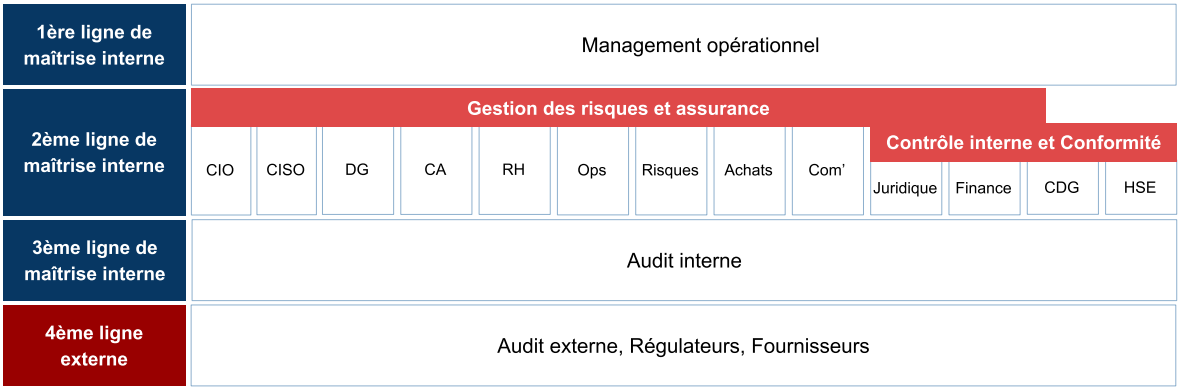


Figure 3 : Les 3+1 lignes de maîtrise de la gouvernance de la sécurité numérique

[9] Le groupe de travail a réalisé une adaptation du cadre conceptuel proposé par l'IIA dans son *Position Paper* de 2020, *The IIA's Three Lines Model - An Update of the Three Lines of Defense*

L'enjeu est de pouvoir prendre en compte l'ensemble des aspects de la sécurité numérique, à la fois au niveau global et transversal, applicable et évolutif, pragmatique et pilotable, tout en rendant compte de la pluralité des contextes stratégiques auxquelles sont confrontées les organisations et de la diversité des réponses qu'elles apportent à cette problématique. Pour faciliter la lisibilité de l'action à mener et la bonne répartition des tâches, la gouvernance de la sécurité numérique se structure donc autour des **3 vecteurs suivants** :

Vecteur 1. Définition de la politique de sécurité numérique (PSN)

Vecteur 2. Application de la politique de sécurité au quotidien

Vecteur 3. Pilotage, suivi par les métriques et communication

L'ensemble des grandes actions à mener et des orientations à arbitrer sur ces vecteurs sont cartographiées ci-dessous, et font l'objet d'un développement dans les sous-parties suivantes.

Piliers de la gestion par les risques de la gouvernance de la sécurité numérique							
Vecteur #1 *Politique de la sécurité numérique*	Définir l'ambition de la gouvernance	Comprendre son activité numérique	Connaître son seuil d'acceptation des risques	Apprécier les risques numériques	Définir sa stratégie et sa valorisation	Définir des polices d'assurance adaptées	Placer l'humain au centre du jeu
Vecteur #2 *Application de la politique au quotidien*	Qualifier ses services numériques critiques	Bâtir sa protection	Orienter sa défense et anticiper sa réaction	Faire preuve de résilience en cas de cyberattaque	Suivi de la conformité réglementaire en interne	Entretien de l'hygiène numérique et des bonnes pratiques	
Vecteur #3 *Pilotage, suivi et communication*	Mesure de la performance	Analyse de la performance	Communication du suivi et de la performance				

Figure 4 : Grandes actions et orientations à arbitrer sur les 3 vecteurs de la sécurité numérique

1.1 VECTEUR 1 - CONSTRUIRE ET ENDOSSER SA POLITIQUE DE SÉCURITÉ NUMÉRIQUE

Le premier vecteur de gouvernance vise à définir et endosser les éléments structurants de la PSN, ou « Politique de Sécurité Numérique ».

1.1.1 DÉFINITION DU CONCEPT DE POLITIQUE DE SECURITÉ NUMÉRIQUE (PSN)

Le terme de **Politique de Sécurité Numérique** (PSN) traduit la nécessité d'élargir le périmètre de protection au-delà des seuls systèmes d'information des organisations et de la classique Politique de Sécurité des Systèmes d'Information (PSSI). En effet, la sécurité numérique englobe aujourd'hui des enjeux plus vastes, à commencer par la maîtrise des dépendances technologiques et de leurs conséquences, qu'elles soient géopolitiques (hybridité de la menace, porosité des intérêts étatiques et crapuleux,...), juridiques (injonctions induites par la portée extraterritoriale des divers droits régionaux) ou économiques (abus de positions dominantes et pratiques anti-concurrentielles…). Elle doit également pouvoir intégrer les défis organisationnels induits par le déploiement des nouvelles technologies comme l'IA et le *Shadow AI*. Les menaces induites sur les fondements de la cybersécurité

(confidentialité, intégrité, disponibilité), ainsi que la conformité, s'étendent donc au-delà de la seule SSI. La PSN vient ainsi englober la PSSI pour aligner la sécurité sur l'ensemble des risques réels de l'organisation en matière numérique. La PSN s'insère de surcroit dans un cadre plus général qui fait de la sécurité numérique un levier de création de valeur en faveur de la résilience des organisations, laquelle résilience est clairement définie sur le plan juridique par un cadre législatif comme la réglementation européen *Digital Operational Resilience Act* (DORA).

1.1.2 DÉPLOIEMENT DE LA PSN EN SEPT ÉTAPES

#1 Dans un premier temps, la construction de la politique de sécurité numérique (PSN) doit être adaptée au périmètre d'action propre à son organisation, c'est-à-dire à son type d'exposition en interne. Véritable cadre de la gouvernance de la sécurité numérique, la PSN doit prendre en compte toutes les entités et filiales de l'organisation et différents secteurs d'activité auxquelles elles contribuent.

De plus, l'effort à engager en matière de sécurité numérique varie considérablement en fonction de la nature des menaces extérieures auxquelles l'organisation doit faire face. Le risque cybercriminel de masse et le risque stratégique constituent deux natures de menaces à gérer de manière différente. Dans l'esprit de la directive européenne NIS2, et de sa future transposition française, un opérateur d'intérêt vital (OIV), une entité importante (EI) ou une entité essentielle (EE) ne se sécurisent pas de la même manière qu'une organisation non-soumise à cette législation, ou une PME. Selon l'exposition à la menace stratégique ou à la menace cybercriminelle et de masse, cette cible de sécurité correspondra à des niveaux différents, allant du niveau basique au niveau élevé, en passant par les niveaux modéré et avancé.

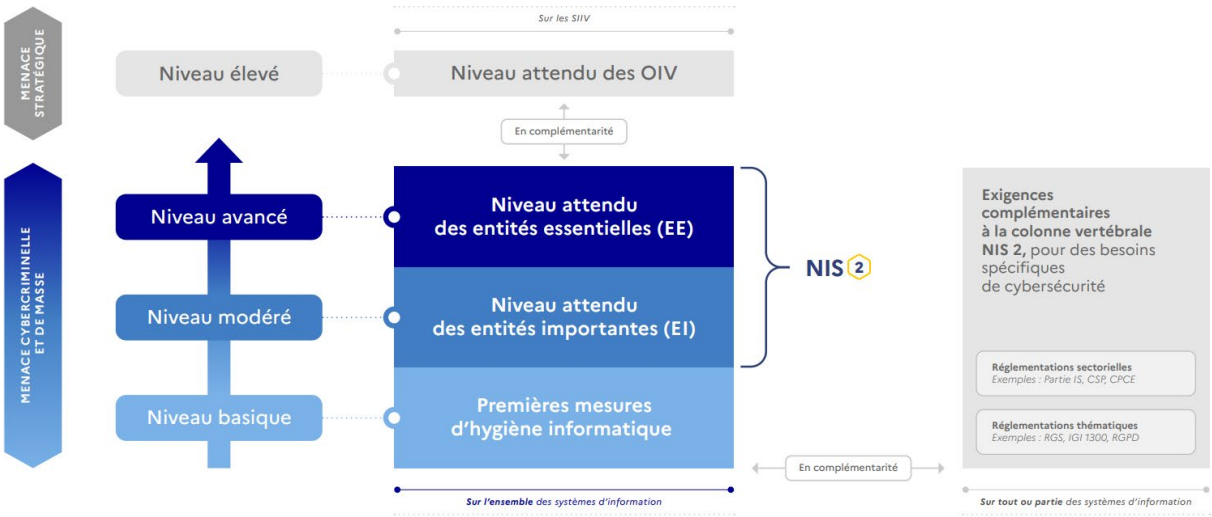


Figure 5 : ANSSI - Présentation du document de travail (ReCyf) en amont de la transposition en droit français de NIS2 (17 mars 2026, Campus Cyber)

L'élaboration PSN doit donc débuter par la définition d'une cible de sécurité ajustée aux expositions internes (périmètre propre) et externes (menaces). Une fois alignée sur le seuil d'acceptation des risques de l'organisation, cette cible devient le cap directeur de la gouvernance de la sécurité.

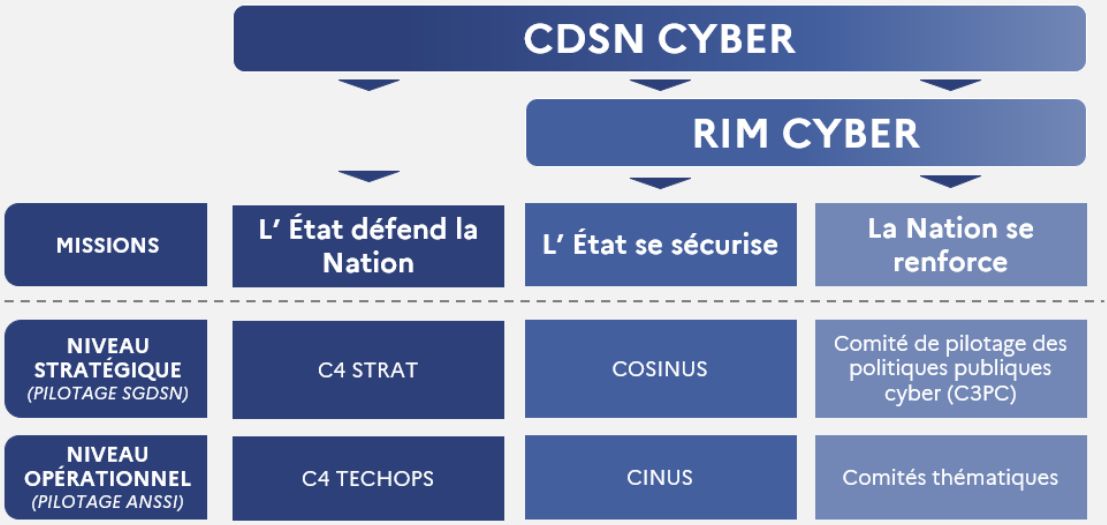
REX ANSSI

Structure et périmètre de la gouvernance de la sécurité numérique pour les besoins propres de l'État français

L'action de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'inscrit dans le cadre stratégique national renouvelé par la Revue nationale Stratégique 2025, et est détaillée opérationnellement, dans son volet cyber, par la Stratégie nationale de cybersécurité 2026-2030 qui fixe la trajectoire de la France pour devenir une Nation cyber de premier rang, capable de protéger durablement ses citoyens, son économie et ses institutions dans un environnement numérique devenu pleinement stratégique.

L'organisation et le périmètre de la gouvernance de la sécurité des systèmes d'information de l'État s'inscrit dans ce cadre stratégique français en matière de cybersécurité. Ainsi, La stratégie nationale de cybersécurité dernier confirme et renforce cette gouvernance autour de deux principes :

- Une séparation des missions offensives et défensives. Les missions défensives relèvent de l'ANSSI en tant qu'Autorité Nationale en matière de cybersécurité et de cyberdéfense ;
- Une gouvernance de la cybersécurité en trois missions :
    1. L'État défend la Nation : connaissance de la menace et élaboration de la réponse de la France aux cyberattaques ;
    2. L'État se sécurise : pilotage de la sécurité des systèmes d'information de l'État et de ses opérateurs les plus critiques ;
    3. La Nation se renforce : coordination de l'action publique et des efforts privés concourant à renforcer la cybersécurité des particuliers, des entreprises, des associations et des collectivités territoriales.



En tant qu'autorité nationale de cybersécurité et cyberdéfense rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDN), l'ANSSI pilote et coordonne la sécurisation des systèmes d'information de l'État au travers une comitologie définie par l'Instruction générale

interministérielle IGI1337. Cette comitologie au niveau opérationnel, stratégique et politique établit annuellement une feuille de route pour la sécurité numérique et contrôle sa bonne mise en œuvre. Cette feuille de route est ensuite déclinée au sein de chaque ministère et dans les établissements publics qui leur sont rattachés, par les fonctionnaires de sécurité des systèmes d'information de ces ministères.

Cette comitologie cyber s'articule avec la gouvernance numérique de l'État, elle-même organisée en niveaux, opérationnel (CINUM) et stratégique (COSINUM), pilotés par la Direction du numérique (DINUM). Cette coordination entre les deux chaînes est primordiale pour assurer la sécurisation de la numérisation des usages de l'État. À ce titre, l'ANSSI est systématiquement sollicitée en tant que conseil dans le cadre des grands projets de transformation numérique de l'État.

Au-delà de la sécurisation des SI de l'État, face à l'évolution de la menace qui touche désormais tous les pans de la société, du citoyen aux entités les plus critiques, l'ANSSI a un rôle de coordinateur des politiques publiques cyber en faveur du renforcement global de la résilience cyber de la nation. Cette action globale requiert une coordination avec l'ensemble de l'écosystème de la cybersécurité et du numérique pour contribuer à faire du risque cyber un risque global pris en compte au plus haut niveau des organisations.

Vincent Strubel, Directeur général de l'ANSSI

 # 2 Dans un second temps, la consolidation du premier vecteur de gouvernance de politique de sécurité numérique (PSN) intègre une compréhension plus fine des activités numériques sur les différents périmètres de l'organisation. On ne sécurise bien que ce que l'on connaît bien et en ce sens, cette étape de recensement de l'activité passe principalement par :

- **L'identification** des valeurs métiers, ressources et biens supports de l'organisation (actifs et systèmes numériques) et l'évaluation de leurs niveaux de criticité pour l'organisation ;
- **La préparation** de la maîtrise des usages numériques (plan de transformation, conduite du changement, montée en compétences et formation continue aux processus et outils) ;
- **La cartographie** de l'écosystème de l'organisation par interactions métier et flux numériques ;
- **La prise en compte du cadre légal**, réglementaire, organisationnel et technologique qui régit les activités numériques de l'organisation ;
- **La mise à jour et l'évaluation** de ces données par la réalisation d'une veille sur les potentielles évolutions de l'ensemble de ces aspects.

 # 3 Dans un troisième temps, la politique de sécurité numérique interroge la définition de l'appétence au risque de l'organisation dans le but de qualifier le seuil d'acceptation des risques numériques, en s'alignant sur la conception globale des risques de l'organisation et les objectifs de sécurité qu'elle s'est fixés. Elle est un élément essentiel pour la gestion de la sécurité numérique par les risques.

 # 4 Dans un quatrième temps, la politique de sécurité numérique prend en compte les résultats de l'identification et la hiérarchisation des risques principaux, selon au moins deux approches :

- **L'approche par l'hygiène numérique et la conformité**, pour les risques les plus vraisemblables et les activités concernées par diverses législations.
- **L'approche par les « scénarios »**, pour se prémunir des attaques plus sophistiquées et ciblant, en priorité, les valeurs métiers[10], ressources et biens supports les plus critiques de l'organisation. Sur chaque scénario, l'analyse des risques passe alors par la construction d'une matrice croisant leurs taux d'occurrence et leurs niveaux d'impact, afin de les hiérarchiser de part et d'autre de la zone d'acceptabilité, de les prioriser et d'en quantifier les différents impacts.

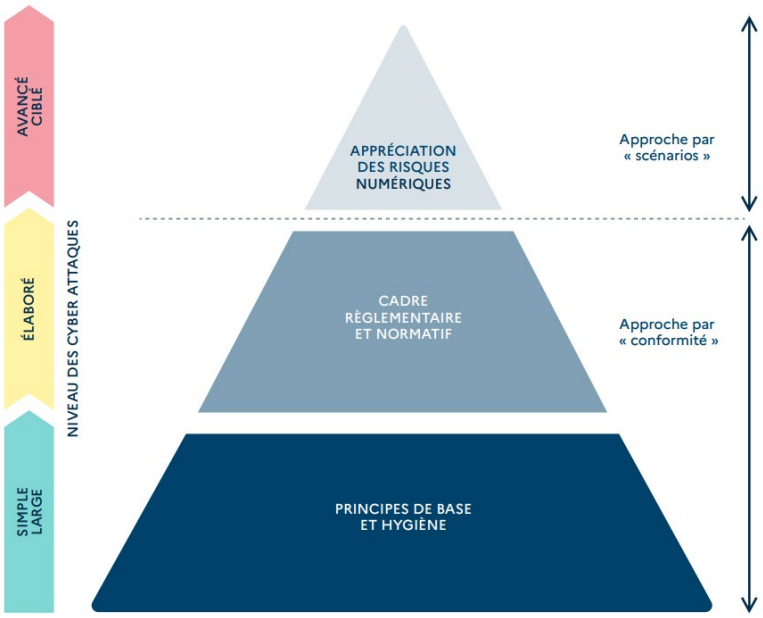


Figure 6 : Méthode de gestion par les risques (EBIOS, Risk Manager – ANSSI)

 # 5 Dans un cinquième temps, vient alors la définition de la stratégie de sécurité numérique, sa valorisation par la communication. Cette étape consiste principalement dans l'analyse et l'arbitrage des risques numériques (comprenant la priorisation et le plan de réduction des risques) et le plan qui en découle de mise en œuvre des mesures de mitigation des scénarios de cyberattaque critiques, avec :

- **La définition et la formalisation d'une «** feuille de route », ou politique de sécurité numérique (PSN), avec **orientations et niveaux d'ambitions applicables** au sein de l'organisation. Cette étape de la démarche implique l'ensemble des parties prenantes (dont le comité exécutif et le conseil d'administration) pour la rendre communicable et congruente avec la gouvernance globale de l'organisation et les responsabilités réellement engagées par les différentes parties prenantes.

[10] Notamment à l'aide d'indicateurs de *Recovery Time Objective* (RTO) et de *Recovery Point Objective* (RPO) associés.

- **L'élaboration d'un plan global d'amélioration continue de la sécurité numérique**, incluant les recommandations de mitigations des risques prioritaires (avec un échelonnement dans le temps et une déclinaison en ressources), ainsi que d'éventuelles démarches d'homologation, de vérification et d'audit de l'application de la politique de sécurité numérique, en veillant à la mise en conformité des SI opérés.

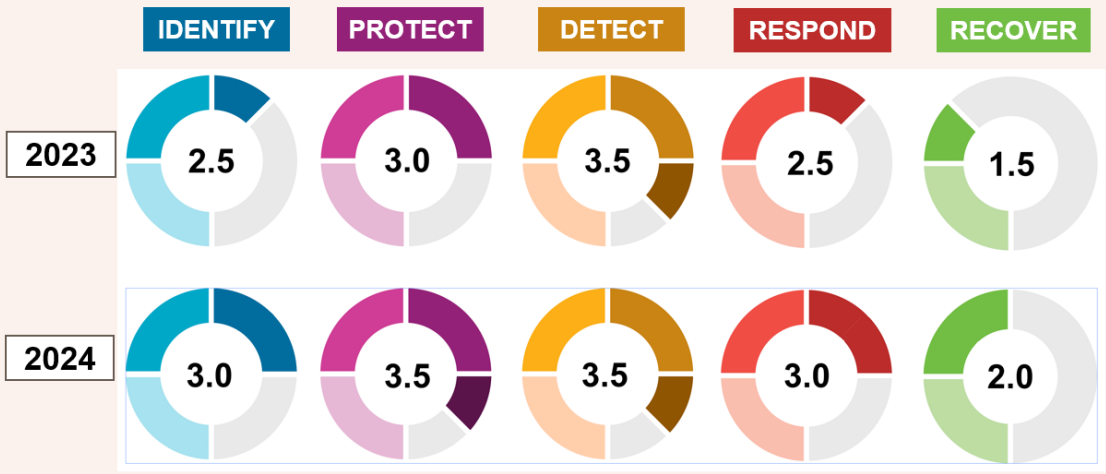
 # 6 Dans un sixième temps, la politique de sécurité numérique doit prévoir l'adoption d'une police d'assurance cyber. Dans la lignée des travaux menés sur la cartographie de la couverture des risques numériques existants, cette police d'assurance doit être adaptée et graduelle pour couvrir les risques résiduels et non encore traités sur les quatre piliers de la prévention, de l'assistance, des opérations et de la responsabilité. La réalisation de cette étape en collaboration avec les *risk managers*, différents courtiers et assureurs, permet d'évaluer la pertinence et la robustesse de la gouvernance dans son ensemble, ainsi que celle des scénarios critiques identifiés analyses d'impacts associées, notamment sous l'angle du portage de risques auprès des tiers (fournisseurs et clients).

REX GETLINK
Décliner sa politique de sécurité numérique
en contrat d'assurance cyber adapté

Dans le but de traduire, sous la forme d'une police d'assurance adaptée, les besoins résiduels qui ne sont volontairement pas pris en charge par notre gouvernance de la sécurité numérique, une matrice de maturité en cybersécurité a été développée. L'approche de l'assurance est globale et couvre l'ensemble des activités du groupe, sans pondération spécifique par segment. L'existence d'un SOC [11] mutualisé conduit à une politique d'assurance unique et globale, plutôt qu'à des polices distinctes par activité.

La grille de maturité se fonde sur une auto-évaluation annuelle de 180 questions permettant principalement de recenser les couches de protection mises en place chez Getlink et de qualifier le niveau d'étanchéité de ces couches. Les réponses sont réalisées en collaboration avec le courtier et viennent attribuer une note de 0 à 4 sur cinq axes couverts par le premier vecteur de gouvernance, allant de l'identification à la récupération, en passant par la protection, la détection et la réponse à incident.

EVOLUTION DE NOTRE MATURITE 2023 / 2024, NOTE ENTRE 0 ET 4

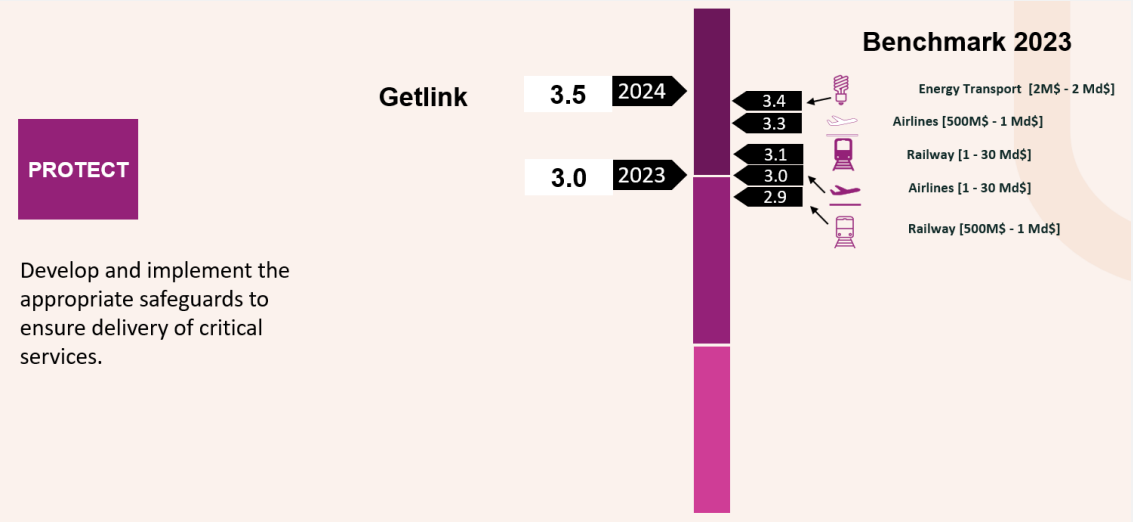


Maintien de notre bon score sur la Detection, progrès dans toutes les autres categories et capacité de Recover en restant très en retrait

L'amélioration continue du score sur ces 5 axes est directement corrélée à l'équivalence entre le risque opérationnel associé à cette notation et le cœur de métier de l'assurance. Cela signifie en pratique qu'un score élevé permet d'améliorer aussi bien la sécurité réelle de l'organisation que l'assurabilité de l'entreprise et, par conséquent, d'en réduire la franchise.

Le courtier réalise, par ailleurs, un benchmark annuel, détaillé par segment d'activité, en s'appuyant sur l'expertise d'une « pratique » d'assurance dédiée.

[11] *Security Operations Center*, organe de surveillance et de détection de la menace. C'est une tour de contrôle qui veille sur les infrastructures 24h/24, souvent opérée par des prestataires ou mutualisée.



Une interrogation s'est initialement posée quant à la possibilité de recourir à d'autres tiers de confiance pour ce type d'évaluation. Cependant les auditeurs se concentrent davantage sur la conformité que sur la maturité et, contrairement à certains acteurs du secteur bancaire, le recours à des services généraux internes n'était pas possible pour fournir des analyses pertinentes en la matière.

Frédéric Riga, Chief Digital Officer chez GETLINK

 # 7 Dans un septième temps, la politique de sécurité numérique s'assure des processus propres à sa coordination et à sa mise en œuvre, en portant une attention particulière aux points de contact avec les autres gouvernances : gouvernance des risques et de la conformité, de la sécurité physique, du numérique de façon plus générale, et gouvernance groupe. La bonne répartition des processus de cette politique et leur mise en visibilité au plus haut niveau de décision auront notamment pour effet connexe d'anticiper la charge mentale et la frustration du RSSI, du DSI et des équipes travaillant à la sécurité numérique.

REX BOSTON CONSULTING GROUP
Structurer sa gouvernance par
une politique et une comitologie partagées

Pour assurer à la politique de sécurité numérique une réalisation performante, des arbitrages éclairés et partagés avec les tiers, une revue par des services d'audit interne ou externe, et un pilotage en amélioration continue avec le soutien d'un organe de surveillance, il est essentiel de lui établir un cadre d'action simple et clair. L'efficacité et la robustesse du dispositif de gouvernance repose en premier lieu sur la bonne désignation contextuelle des acteurs à responsabiliser, à informer et à rassembler entre :

- **Le comité stratégique,**
  - En charge de définir les orientations stratégiques et de prendre les décisions finales concernant la sécurité numérique à l'échelle du groupe.
  - Composé principalement des différents dirigeants métiers et numériques des entités, des directeurs financiers, juridiques, risques, conformité, audit interne, numériques et cyber au niveau groupe. Un deuxième dispositif stratégique parallèle peut intégrer les membres du conseil d'administration et la direction générale.
  - Réuni pour la revue des orientations et la surveillance de la performance tous les 6 mois.
- **Le comité de pilotage**,
  - En charge d'arbitrer, d'orchestrer et de faire réaliser les décisions clés prises à l'échelle des organisations, en donnant les orientations à décliner dans les différentes entités.
  - Composé principalement des directeurs numérique et cyber groupe, des directeurs métiers, des directeurs numérique et cyber des entités.
  - Réuni pour la revue des orientations et la surveillance de la performance tous les 2 mois.
- **Le comité de direction**,
  - En charge de l'application et de la gestion de la gouvernance de la sécurité numérique du groupe.
  - Composé principalement du directeur cyber au niveau groupe et des directeurs métiers et cyber des entités.
  - Réuni pour le pilotage, la mesure et l'analyse de la performance tous les mois.

Jean-François Bobier, Partner & VP Product Management

Adnène Trojette, Principal chez BCG Paris Cyber

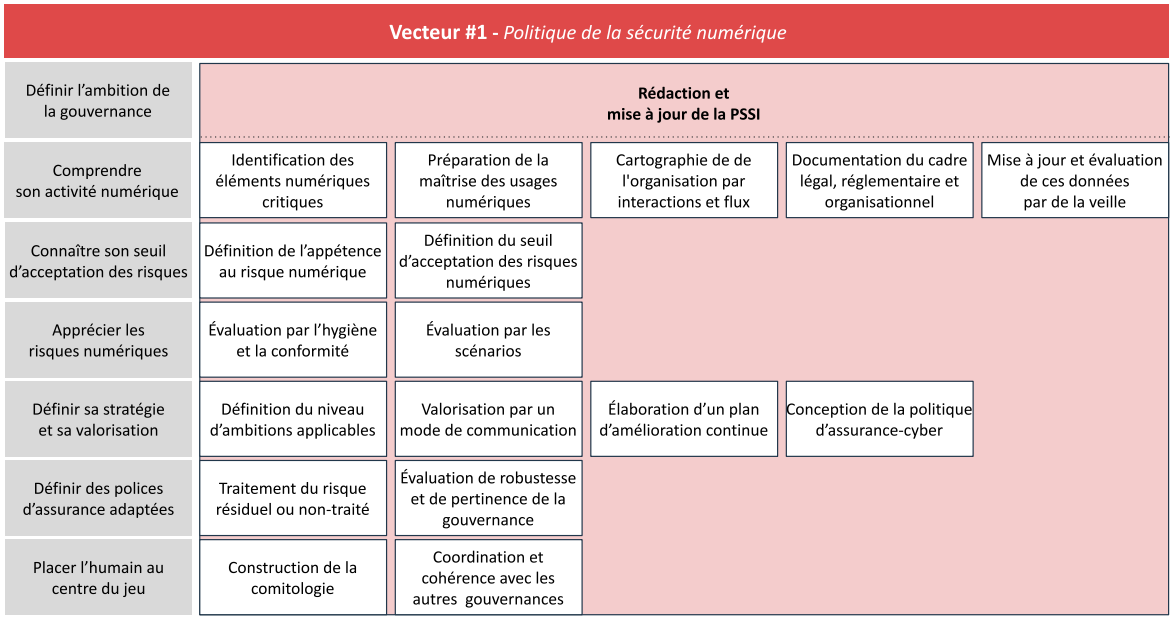


Figure 7 : Synthèse - Grandes actions et orientations à arbitrer sur le vecteur #1

1.2 VECTEUR 2 - VEILLER À L'APPLICATION AU QUOTIDIEN DE LA POLITIQUE DE SÉCURITÉ NUMÉRIQUE

Une fois la politique de la sécurité numérique structurée, et pour ne pas rester lettre morte, la gouvernance doit pouvoir s'instancier via un partage concerté des responsabilités et leur éventuelle délégation. Le deuxième vecteur de gouvernance porte donc sur la mise en pratique et l'application au quotidien des responsabilités afférentes à la sécurité numérique. Il consiste à mettre en place :

- **Une déclinaison organisationnelle avec la composition d'équipes dédiées à la sécurité numérique.** Celle-ci se fait selon les besoins et la maturité de l'organisation et associe un descriptif de poste aux différentes fonctions requises, *a minima* pour les compétences suivantes :
  - Les opérations de sécurité du SI existant, de sécurisation des développements, de résolution de problèmes et de test ;
  - L'administration de la sécurité, l'homologation et la mise en conformité ;
  - La gestion des risques numériques.
- **Une garantie de la sécurité numérique sur tous les cycles de vie,** ce qui implique de :
  - Veiller, avec les fournisseurs, à la conception native de la sécurité numérique des produits ;
  - Mettre à jour régulièrement l'analyse de l'exposition externe (état de la menace, cadres réglementaires) ;
  - Mettre à jour régulièrement l'analyse de l'exposition interne (criticité de son patrimoine numérique, changements techniques ou stratégiques) ;

- Bâtir et entretenir de manière adaptée sa protection applicative, système, réseaux et physique ;
- Orienter sa défense par une meilleure détection des chemins d'attaques et une journalisation des accès aux SI, et anticiper sa réaction par un entraînement à la qualification des cyberattaques ;
- Faire preuve de résilience en cas de cyberattaque, suivre la mise en conformité réglementaire en interne, en intégrant notamment la capacité à produire une « alerte précoce » sous 24 heures en cas d'incident majeur (obligation NIS 2), ce qui impose une refonte des processus de remontée d'information, mais également de l'activation de la cellule de crise aux entretiens avec les autorités et les assureurs, en passant par la gestion de la communication et les PCA / PRA.

- **Une organisation de campagnes de formation, de communication, de sensibilisation, d'acculturation** des différentes parties prenantes par :
  - La diffusion du règlement intérieur, de la charte cybersécurité, des sanctions disciplinaires, des bonnes pratiques aux collaborateurs et usagers ;
  - La prévention de son écosystème direct et de ses différentes parties prenantes (fournisseurs, sous-traitants, clients, partenaires,…) ;
  - La formation continue interne (académies, webinaires, MOOC etc.) ou en faisant venir des externes, la montée en compétence ou la réutilisation des compétences pour les équipes dédiées (plans d'acquisition et maintien des compétences) ;
  - Les entraînements réguliers à des scénarios de crise, jeux de rôle, hackathons etc.

Vecteur #2 - *Application de la politique de sécurité au quotidien*					
Décliner au plan organisationnel la PSN	Corrélation des besoins fonctionnels, compétences et RH				
Garantir la sécurité numérique sur tous les cycles de vie	Analyses de l'exposition interne (patrimoine, changements)	Analyses de l'exposition externe (état menace, cadre réglementaire)	Construction, entretien de sa protection	Orientation de sa défense et anticipation de ses réactions	Faire preuve de résilience en cas de cyberattaque
Former, communiquer, sensibiliser, acculturer	Diffusion de bonnes pratiques et normes	Prévention des tiers (fournisseurs, clients)	Formation continue en interne	Entraînements réguliers de scénarios de crise et jeux de rôle	

Figure 8 : Synthèse - Grandes actions et orientations à arbitrer sur le vecteur #2

REX GROUPAMA

L'équilibre de la mise en application de la sécurité numérique

En temps de « *run* », l'application au quotidien de la politique de sécurité numérique au sein du groupe Groupama passe par l'animation de la filière dédiée à la SSI. La Commission de Sécurité Groupe (**CSG**) est chargée de l'orchestration de cette filière et joue, en s'appuyant sur des groupes de travail communautaires, le rôle d'un organe d'orientation. Elle est également le lieu de revues d'incidents, et plus généralement de contrôle des KPI opérationnels.

Le RSSI du Groupe rend compte de la maîtrise du risque de sécurité numérique auprès du Comité des Risques Opérationnels Groupe (CROG), aux côtés de la Direction des Risques Groupe. La sécurité numérique y est bien identifiée comme un risque majeur, parmi les autres risques revus tous les semestres dans cette sous-instance du Comex.

> *Il est à noter que le RSSI est principalement chargé de l'articulation entre la politique de gouvernance, la gestion des processus organisationnels, et la mise en œuvre des normes de sécurité au niveau groupe et dans chaque entité. Sur le plan organisationnel, la sécurité numérique est attachée au DG du GIE et au Directeur des risques du groupe (CRO).*

Les arbitrages de mutualisation des actifs sont une dimension essentielle du rôle pivot assumé par la sécurité numérique :

- **Sur le périmètre français**, 80% du numérique se trouve déjà mutualisé, répondant à une logique de rationalisation économique et humaine pour assurer des fonctions clés comme le SOC [12] et le CSIRT [13].
- **À l'international**, et en particulier suite aux processus de rachats, seule la sécurité numérique se trouve mutualisée, tandis que les systèmes d'information restent spécifiques à chaque pays. Cette pratique propre à la sécurité numérique s'inspire du dispositif français touchant à la partie supervision d'une activité réglementée.

  Ainsi, tout en gardant un numérique strictement cloisonné à l'international, chaque entité opère comme si elle était une entreprise indépendante de toute maison mère. Sur le périmètre de la sécurité numérique, en revanche, le groupe assure la supervision H24/7 de la sécurité des filiales de l'international sur le modèle mis en œuvre en France.

  Le rattachement organisationnel de la sécurité numérique au sein de l'IT Groupe, doublé d'un lien fonctionnel avec la Direction des Risques, favorise par ailleurs une harmonisation des niveaux de sécurité cohérente avec le caractère mutualiste du Groupe.

En temps de « crise », la nécessité d'arbitrer stratégiquement entre temps court et temps long est aussi importante que de lutter opérationnellement contre les réparations prématurées effectuées au profit du maintien de la qualité de service, mais nuisant à la phase d'investigation de l'attaque.

L'anticipation et l'exercice, en temps d'accalmie, des mandats de crise et des délégations éventuelles de responsabilité orientent l'application claire et partagée au quotidien de la sécurité numérique. Sur ces sujets, des exercices sont régulièrement conduits pour assurer la bonne compréhension des processus et leur bonne exécution par toutes les parties prenantes.

Au sein de Groupama, la sécurité numérique étant positionnée au niveau groupe, le RSSI Groupe est chargé de la cellule de crise opérationnelle (avec équipes tech G2S, et celles des entités impactées) pour assurer la gestion concrète des opérations. Une cellule distincte assure la prise des décisions et la communication avec les parties prenantes. Le RSSI Groupe assure la liaison entre les deux cellules.

Patrick Prosper, DSES - RSSI Groupe chez GROUPAMA

[12] *Security Operations Center* (SOC), organe de surveillance et de détection. C'est une tour de contrôle qui veille sur les infrastructures 24h/24, souvent opérée par des prestataires ou mutualisée.

[13] *Computer Security Incident Response Team* (CSIRT), organe de réaction et de coordination. Il intervient en cas d'incident avéré pour gérer la crise et assurer le partage d'informations.

Trois échelles de CSIRT existent : **le CSIRT d'entreprise** (unité interne dédiée à la réponse à incidents dans l'organisation), **le CSIRT régional / sectoriel** (centre de proximité créé par le plan France Relance pour accompagner principalement PME et collectivités, en relais vers l'ANSSI), **le CERT-FR** (CSIRT national opéré par l'ANSSI pour les incidents d'ampleur nationale et qui coordonne la réponse étatique).

REX AIRBUS
L'intégration native de la sécurité numérique
au plus haut niveau de direction

L'application de la politique de sécurité numérique et le maintien opérationnel de la continuité de service se découpe en deux catégories de gestion :

- L'analyse et la détection de risques, qui est intégrée à la gestion normale du *run*.
- La gestion de crise à proprement parler, avec ses deux chaînes de commandement distinctes (périmètre avion et hors avions de tous ordres).

La nature des activités industrielles d'Airbus pousse à l'intégration native de la sécurité au plus haut niveau de direction.

La gouvernance est mise en musique par une double chaîne ascendante et descendante :

- D'une part, grâce à la remontée d'informations sur l'ensemble des actifs opérationnels à destination des directions métiers, puis à celles du *Chief Security Officer* (CSO) et du *Corporate Security Council* (CSC) qui viennent alimenter le *Chief Executive Officer* (CEO) et les différents boards ;
- D'autre part, selon les feuilles de routes stratégiques qui donnent la vision, les orientations du groupe et les principes d'action **pour les instances de sécurité de chacune des divisions** (filiales et *supply* comprises, malgré quelques superpositions), **avec réplication régionale** sur le modèle de la structuration géographique du groupe (5 zones mondes en dehors des 4 pays cœur), **afin d'irriguer *in fine* le quotidien des métiers de manière transversale** (structurés pour la sécurité numérique autour d'un *Chief Information Security Officer* (CISO) par division, et d'un CISO Group et d'un SOC très majoritairement internalisé).

Le CSO est exposé sur les 4 chaînes de *Plan-Do-Check-Act* sur l'ensemble des actifs avec un rôle d'*Accountable* sur l'ensemble des phases.

La DSI est exposée sur la phase *Plan-Do* :

- **Le DSI étant *Responsible* sur le *Do*** (designer et fabriquer les produits et les services, avec responsabilité pénale pour les organisations approuvées).
- **Le CISO Groupe et le responsable de la gouvernance de la sûreté Group étant *Responsible* sur le *Check-Act***, notamment sur la partie de mitigation mutualisée (avec un CERT, un SOC non-national et quelques SOC nationaux, un Red Team Group, une entité pour les architectures cyber).

Anne Tricot, Chief of Staff at Head of CSO

Michael Barthellemy, OCSSI Airbus Commercial

Olivier Pujol, VP Governance, Risk & Compliance at Airbus

1.3 VECTEUR 3 - PILOTER LA SÉCURITÉ NUMÉRIQUE PAR LES MÉTRIQUES ET COMMUNIQUER À BON ESCIENT AUX DIFFÉRENTES PARTIES PRENANTES

Le troisième vecteur de gouvernance permet d'exercer un retour sur la structure et l'application des principes de sécurité numérique. Le pilotage par les métriques couvre l'ensemble des capacités de résilience offertes par la sécurité numérique (capacités d'anticipation, d'adaptation, d'absorption, de reconstruction). Il s'appuie notamment sur plusieurs points.

- **La mesure de la performance**, passant par un outillage du pilotage et du suivi de l'application de la politique de sécurité numérique (gestion des risques, menaces, attaques, réponses à incident) ;
- **L'analyse et la comparaison de la performance**, passant par un rapport évaluant l'atteinte des objectifs fixés par les ambitions de la politique de sécurité numérique ;
- **La présentation de la performance**, passant par la création de rapports synthétiques, adaptés aux besoins en information, en appropriation et en engagement, des différents interlocuteurs et aux besoins des comités.

Pour faire du pilotage par les métriques un levier d'amélioration réel du dispositif de la sécurité numérique, la mise en place de bonnes pratiques doit se porter sur deux plans :

- **D'une part, l'expression et la traduction en un langage commun (objectifs, critères, vocabulaire) des besoins des différentes parties prenantes**, à décliner ensuite en métriques. Ce premier plan tient à la définition des besoins et passe par une approche réaliste qui veille à assurer un niveau de protection :
  - Cohérent pour le seuil d'acceptation du risque et la couverture effective ;
  - Compétitif par rapport aux autres acteurs du secteur.
- **D'autre part, la construction des outils de mesure adaptés** pour disposer de données fiables, et de moyens de calculs suffisamment précis et exacts, permettant de fluidifier la gouvernance en faisant remonter le type et le degré d'information requis au bon niveau de décision, selon les différents comités mis en place :
  - **Pour le comité stratégique**, focalisé sur les risques majeurs, le pilotage par les métriques se traduit par le suivi d'une dizaine de KPIs de synthèse qui donnent à voir :
    - **Quelques éléments de tendances et menaces macro** [14] pertinentes pour les spécificités du contexte organisationnel ciblé.
    - **Les risques majeurs de sécurité numérique** identifiés dans l'analyse des risques par scénarios (avec évaluation qualitative et déclinaison quantitative des impacts).
    - **L'état de maturité moyen pour chaque catégorie d'action de sécurité numérique** (identification, protection, détection, réponse et remédiation).

[14] Cf les échanges des CSIRT, travaux de *Cyber Threat Intelligence* de CERT-FR ou le rapport annuel *Panorama de la menace* réalisé par l'ANSSI

- **La fenêtre critique de vulnérabilité**, par ratio de la surface d'exposition et du taux de couverture sur des actifs positionnés au-delà du seuil d'acceptabilité du risque ou des exigences de conformité nécessaires.
- **Les objectifs visés sur ces KPI et les grandes lignes du plan d'action associé,** avec déclinaison temporelle possible à l'horizon de la prochaine réunion de revue stratégique, à l'horizon annuel et à l'horizon de la feuille de route pluriannuelle (3-5 ans).

- **Pour le comité décisionnel**, focalisé sur la performance du programme de sécurité numérique, le pilotage par les métriques se traduit plutôt par un ensemble de KPIs présentés sous la forme d'un tableau de bord de synthèse des différents projets, qui donne à voir :
  - **Le suivi des investissements et la performance de la transformation**, via la consolidation de l'avancement des différents projets à l'état de portefeuille de programmes. L'objectif n'est pas de suivre les tâches, mais d'abord d'avoir une vue d'ensemble pour s'assurer que les budgets alloués se traduisent par une délivrance effective de nouvelles capacités de sécurité numérique aux échéances promises aux comités exécutifs et conseil d'administration.
  - **L'efficacité du dispositif de résilience et la maîtrise de l'impact métier**. L'objectif est d'évaluer le retour sur investissement des capacités de défense en mesurant concrètement la vitesse à laquelle l'organisation sait absorber ou restaurer les opérations suite à un incident relativement critique.
  - **Le suivi des tendances macro d'exposition au risque et de gestion de la « dette de sécurité »**. La revue trimestrielle des vulnérabilités majeures est ainsi l'occasion d'évaluer la pertinence de nouveaux arbitrages budgétaires ou humains à prendre en compte et à réaliser pour faire converger l'organisation vers les objectifs fixés (réallocation de ressources, acceptation temporaire d'un risque critique, accélération ou arrêt de projet etc.).
- **Pour le comité opérationnel**, focalisé sur la maîtrise des risques opérationnels au quotidien, le pilotage par les métriques donne à voir les résultats terrain de :
  - **L'avancement concret de la feuille de route des projets de sécurisation,** illustré par exemple par un taux d'avancement des tâches techniques ou la répartition du statut d'avancement pour chaque projet au sein d'un programme donné au regard de l'utilisation des ressources humaines et financières.
  - **La maîtrise de la « dette de sécurité » technique**. L'objectif est alors de s'assurer que son organisation répare les trous plus vite qu'ils n'apparaissent, en intégrant une obligation de maintenance de sécurité sur l'ensemble du cycle de vie des produits (conformément à l'esprit du *Cyber Resilience Act*), dans le but de ne pas laisser la situation se dégrader par accumulation ou vieillissement critique de failles non corrigées.
  - **La réactivité opérationnelle face aux alertes**, avec l'évaluation de la vitesse quotidienne à laquelle les équipes techniques traitent les incidents et vulnérabilités de sécurité.

La création de tableaux de bord de suivi n'est pas suffisante à la gestion de la performance et à son partage. L'enjeu principal du pilotage par les métriques est d'arriver à créer un canal de communication et un langage commun avec les trois comités (stratégique pour les CA/DG, décisionnel et opérationnel), pour relever les défis au bon niveau et transmettre les informations nécessaires à la prise de décision au profit d'une amélioration réelle de la valeur créée par l'organisation. L'inscription de la sécurité numérique dans une approche de gestion par les risques (réputationnels, stratégiques, financiers, organisationnels et humains, au-delà de la seule observation de la réglementation) est un premier moyen, l'étude de son impact sur la continuité d'activité et la résilience au service de la performance et la compétitivité en sont un autre.

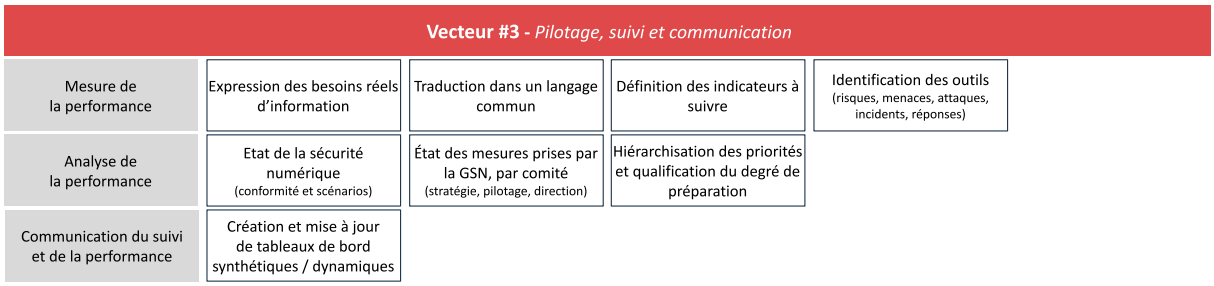


Figure 9 : Synthèse - Grandes actions et orientations à arbitrer sur le vecteur #3

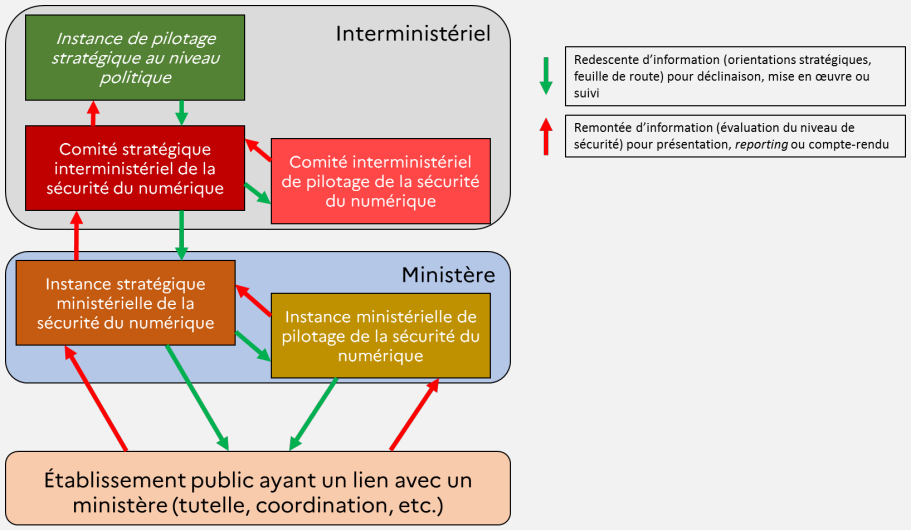
REX ANSSI
Organisation des instances de la gouvernance de la sécurité numérique de l'État

Dans le cadre du Comité stratégique interministériel de la sécurité numérique (COSINUS), le directeur général de l'ANSSI présente un état de la menace relative à la sécurité numérique. Il définit avec les autres membres du comité les orientations stratégiques en matière de sécurité numérique et la feuille de route associée qui seront présentées en instance stratégique de niveau politique, à l'initiative du Premier ministre. Un rendez-vous annuel au minimum est fixé pour chacune des deux instances mentionnées.

Dans le cadre du Comité interministériel de pilotage de la sécurité numérique (CINUS), le directeur général de l'ANSSI suit, en tant que président du comité, la mise en œuvre de la feuille de route validée lors de l'instance stratégique de niveau politique, en proposant une instance de partage et de réflexion sur les difficultés éventuellement rencontrées et l'actualité relative à la sécurité numérique. Un rendez-vous mensuel au minimum est fixé pour cette instance.

Sur invitation des ministères, l'ANSSI est également conviée aux instances stratégiques ministérielles de la sécurité numérique qui déclinent sur le plan organisationnel et opérationnel ce cadre de la gouvernance, à partir d'une organisation cible.

Ces trois instances ont pour but de couvrir l'ensemble des besoins en sécurité numérique des domaines interministériels et ministériels, tant au niveau stratégique et qu'opérationnel.



Vincent Strubel, Directeur général de l'ANSSI

2 RESPONSABILITÉS DES INSTANCES DÉCISIONNELLES POUR UN ALIGNEMENT DES ORIENTATIONS STRATÉGIQUES

2.1 MISE EN COHÉRENCE DES GOUVERNANCES

Au-delà de sa seule dimension technique, la sécurité numérique s'affirme aujourd'hui potentiellement comme un atout stratégique différenciant, ou comme le pilier d'une activité de confiance. La montée en maturité des modèles de gouvernance de la sécurité numérique se mesure donc, même dans des environnements très réglementés, au passage d'une logique de « défense » - souvent réactive, cloisonnée et centrée sur la seule conformité - à une posture de « maîtrise » étendue et proactive. Ce changement de paradigme vise à acquérir une disposition habituelle de résilience numérique, permettant non seulement de subir moins passivement les chocs, mais de maîtriser de manière réaliste l'avenir numérique de l'organisation. Cette résilience se construit selon un double mouvement :

- **Un volet préventif, visant à préserver et sécuriser l'existant** (croissance et actifs) par des capacités d'absorption et de reconstruction rapide. L'enjeu est alors d'assurer la continuité et la qualité de ses fonctions et activités critiques face aux perturbations de toute nature (aléas climatiques, tensions géopolitiques, défaillances tiers).
- **Un volet proactif, visant, sans contre-attaque offensive, à entreprendre pour l'avenir** en façonnant les conditions d'une création pérenne de valeur par des capacités d'anticipation et d'adaptation. L'enjeu est de transformer, autant que possible, les risques numériques en opportunités (économiques, réglementaires, technologiques, géopolitiques, sociales et environnementales) au profit de de l'organisation, de la filière numériqueet du pays d'implantation.

Pour assurer concrètement cette mise en cohérence, il apparaît essentiel :

- **Premièrement, d'intégrer la sécurité numérique dans la cartographie globale des risques de l'organisation**. En effet, le risque en matière de sécurité numérique ne doit pas être considéré isolément, mais comme un facteur aggravant pour les autres risques opérationnels, réputationnels, financiers. Cette démarche implique de répondre aux attentes des autres départements, tant en termes de responsabilité légale que d'implication opérationnelle. Cet alignement est d'autant plus important à l'heure où s'affirme un continuum de la menace numérique, cyber, informationnelle, cognitive et physique. Ce continuum, démultiplié par les capacités de l'intelligence artificielle, expose désormais les organisations à une industrialisation des attaques en ingénierie sociale, risque numérique autrefois réservé à un nombre beaucoup plus restreint de cibles.
- **Deuxièmement, d'analyser les influences des autres actifs métiers de l'organisation sur la sécurité numérique.** Cette démarche est indispensable pour pondérer correctement les interdépendances avec les autres départements et intégrer, le cas échéant, une lecture géopolitique des menaces. Pour certaines activités critiques, notamment celles situées à la

confluence de la sécurité numérique et de la sûreté physique, cette exigence de cohérence peut aller jusqu'à imposer des stratégies de cloisonnement des risques opérationnels, passant par une politique de décentralisation voire un découplage local des actifs.

En sécurité numérique, la résilience des organisations dépend donc autant de la pertinence et de la lisibilité de l'action technique recherchée que de la relation de confiance qui se noue entre les parties prenantes engagées. Les capacités proactives d'anticipation [15] et d'amélioration [16] de la gestion de crise doivent à ce titre se travailler en « temps calme » avec les équipes dédiées afin de préparer en amont, les interactions techniques et psychologiques avec les plus hauts niveaux décisionnaires. Le défi est d'arriver à créer les conditions d'une gestion des perturbations majeures qui soit la plus apaisée et rationnelle possible.

Ce niveau de préparation exige en particulier que le dialogue soit établi, nourri et enrichi au bon niveau, tout particulièrement avec les conseils d'administrations et les comités exécutifs. L'importance actuelle de ces enjeux ne peut plus se satisfaire d'une prise en compte superficielle ou d'une seule revue annuelle pour en permettre la bonne compréhension. En outre, plus les automatismes sont assimilés par exercices en commun, plus ils permettent une gestion limitant les différents effets des cyberattaques (dommages et pertes directes de tous ordres, dégradation longue des performances du patrimoine numérique, effets post-traumatiques). Pour les dirigeants, la partie proactive (capacités d'anticipation et d'adaptation) de la gouvernance de la sécurité numérique repose sur plusieurs piliers :

- **Une architecture de crise claire qui distingue plan stratégique et plan technique :** il est crucial de ne pas improviser l'organisation à mettre en place et de distinguer formellement la cellule décisionnelle (acteurs majeurs de la fonction sécurité numérique) de la cellule opérationnelle (experts en analyse et rétablissement).
- **Des processus de coordination préétablis :** l'efficacité repose sur la définition préalable des rôles, des seuils d'alerte et des canaux de communication sécurisés (notamment une « ligne rouge » pour déclencher l'alarme sans dépendre du SI compromis).
- **Une gestion humaine et communicationnelle :** il est nécessaire d'adopter une transparence proactive envers l'écosystème pour préserver la confiance et, en cas de crise de longue durée, de prévoir le soutien logistique et psychologique des équipes.
- **Le maintien de l'énergie, de l'hygiène numérique :** au-delà de la gestion de l'événement, la gouvernance doit veiller à ce que l'effort de sécurité ne cible pas uniquement les instances décisionnelles, mais irrigue toutes les strates de l'entreprise sur le long terme, afin d'éviter que des failles basiques ne réapparaissent par lassitude ou négligence.
- **L'entretien et l'amélioration continue des capacités de remédiation :** en cas de compromission par l'attaquant, les capacités de remédiation s'avèrent très importantes, afin d'être en mesure de reprendre le contrôle rapidement sur les actifs atteints, notamment pour les actifs les plus critiques de son organisation.

[15] Voir le rapport Cigref, *Anticiper les cyberattaques*, Mars 2024
[16] Voir le rapport Cigref, *Réagir à une cyberattaque massive*, Février 2023

De manière globale, l'intégration réussie de la gouvernance de la sécurité numérique ne peut donc se concevoir isolément. Elle exige une mise en cohérence profonde avec les autres instances et orientations de gouvernance de l'organisation. Quel que soit le modèle de gouvernance de la sécurité numérique, les responsabilités des organes principaux de gouvernance (direction générale et conseil d'administration) restent inchangées. Le modèle des trois lignes de maîtrise [17] fournit à cet égard un cadre robuste. Il rappelle que l'organe de gouvernance (le conseil d'administration) conserve la responsabilité ultime de s'assurer de l'adéquation des structures et processus, ainsi que de l'alignement des objectifs avec les intérêts des parties prenantes. Concrètement, cet organe délègue les ressources au management pour la réalisation des objectifs - tout en veillant au respect des exigences éthiques et réglementaires - et supervise une fonction d'audit interne indépendante pour garantir la confiance.

Comme évoqué dans la première partie de ce rapport, les bonnes pratiques du groupe de travail suggèrent que la cadre d'une gouvernance de la sécurité numérique mature comporte trois niveaux distincts de comitologie, dédiés aux enjeux stratégiques, organisationnels et opérationnels. De la sorte, les principes de gouvernance intègrent nativement une **distinction entre l'approbateur** d'une gestion des risques numériques, **le responsable** de sa structuration et de son pilotage, **l'expert** qui a la connaissance requise pour réaliser le projet de cartographie de la sécurité numérique, et **l'acteur tiers consulté ou informé** - tout particulièrement lorsque ce tiers est un fournisseur critique, avec qui il faut être en mesure de construire un dispositif en miroir d'anticipation et d'adaptation à la crise.

Cette démarche d'application et d'animation de la gouvernance prend une dimension très concrète en se déclinant sous la forme d'un RACI pour chacun des trois vecteurs (définition de la politique de sécurité numérique, application au quotidien et pilotage par les métriques). L'objectif est de pouvoir clarifier sans ambiguïté qui est *Accountable* (responsable ultime), *Responsible* (réalisateur), *Consulted* et *Informed* et sur quel périmètre.

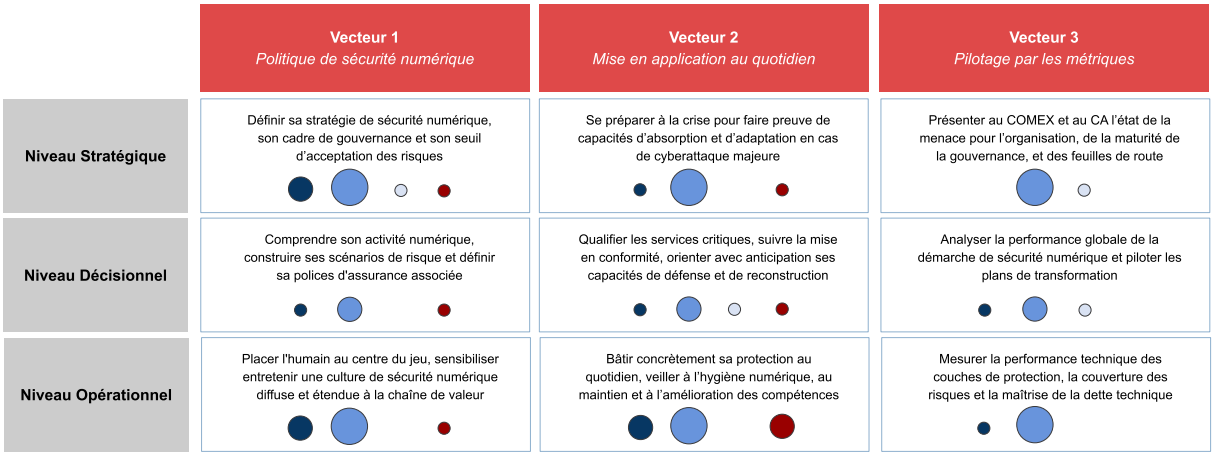


Figure 10 : Synthèse - Implications des différentes parties prenantes

[17] Pour rappel, le groupe de travail du Cigref a appliqué les trois lignes de maîtrise de *l'Institute of Internal Auditors* (IIA) à la sécurité numérique de la manière suivante : première ligne portant sur le management opérationnel, deuxième ligne sur les fonctions support et la gestion des risques, troisième ligne sur l'audit audit interne. Une quatrième ligne externe a été ajoutée à la catégorisation et rassemble les différents fournisseurs, régulateurs et acteurs de l'audit externe.

2.2 IMPLICATIONS POUR LE CONSEIL D'ADMINISTRATION : ORIENTATION, ASSOCIATION ET REMONTÉE D'INFORMATION

Afin que la sécurité numérique s'affirme comme un véritable levier de compétitivité et de performance, les conseils d'administration, et leur président en premier lieu, ont un rôle moteur d'orientation stratégique à exercer.

Positionnés le plus souvent en tant que responsables et approbateurs (*Accountable* au sens d'une matrice RACI), la mission des Conseils ne relève pas de la conduite opérationnelle du dispositif (*Command & Control*), mais de l'orientation, de la validation et de la revue des trajectoires prises, ainsi que de la garantie de l'adéquation des ressources et moyens alloués. Il est à noter que l'entrée en vigueur fin 2024 de la directive européenne NIS2 introduit une obligation pour les organes de direction de suivre une formation (Art. 20.2) leur permettant d'acquérir les compétences suffisantes pour identifier les risques et évaluer les pratiques de gestion des risques de sécurité numérique. Cette obligation accompagne l'engagement de la responsabilité légale des administrateurs en ce qui concerne l'approbation et la supervision des risques en matière de sécurité numérique (Art. 20.1).

Le *vade-mecum* ci-dessous se veut une proposition de synthèse des responsabilités attendues des administrateurs en matière de sécurité numérique.

2.2.1 CONTRIBUTION À LA CONSTRUCTION DE LA PSN - VECTEUR #1

Les conseils d'administration sont tout particulièrement attendus pour :

- **Fixer le cap stratégique de la politique de sécurité numérique (PSN).** Les prérogatives des administrateurs concernent l'élaboration des orientations stratégiques de la feuille de route pluriannuelle (3 à 5 ans) et la validation de sa formalisation.

  Portant la responsabilité ultime (*Accountable*) de ces orientations, il incombe à cette instance non-exécutive d'exiger des autres parties prenantes une stratégie unifiée déclinant la mise en œuvre de mesures de mitigation (via un Plan d'Amélioration Continue de la Sécurité, ou PACS, assorti de démarches d'homologation). Pour ce faire, le Conseil doit s'assurer de l'adéquation des ressources financières, humaines et techniques disponibles.

  Le Conseil doit, enfin, impulser la valorisation de cette sécurité numérique par une communication ciblée, afin de transformer la résilience de l'organisation en un véritable avantage concurrentiel.

- **Mettre en cohérence l'objectif visé par la PSN avec l'appétence au risque de l'organisation dans son ensemble.** Le Conseil doit déterminer ce qui est acceptable pour la survie du modèle d'affaires, sans se contenter d'être informé des menaces.

  Pour identifier les arbitrages les plus résilients possibles, la prise de décision doit se fonder, en interne, sur la capacité réelle des mesures en place à anticiper et entraver les attaques, et à absorber et surmonter leurs effets.

  Pour rendre réalistes ces arbitrages, le Conseil doit exiger une remontée d'information transparente et qualifiée, permettant de croiser la vraisemblance et l'impact des pires scénarios d'attaque.

La validation du niveau d'engagement requis nécessite d'interroger les :

- Seuils de risques résiduels raisonnables (appétence)
- Impacts *maxima* acceptables (tolérance)
- Objectifs de mise en conformité (ressources)
- Plans et méthodes de gestion du risque (diminution et politique de transfert vers le marché de l'assurance).

Cette démarche doit être pensée de façon globale, incluant les différentes parties prenantes concernées (*Risk Manager*, fonction numérique, audit interne et externe, courtier et assureur *a minima*).

2.2.2 MISE EN APPLICATION AU QUOTIDIEN - VECTEUR #2

En cas d'incident majeur, le conseil d'administration est attendu pour :

- **Incarner la gouvernance et la résilience en temps de crise.** Les administrateurs ne gèrent pas l'incident technique, mais intègrent la cellule de crise décisionnelle. Il leur incombe de prendre des arbitrages parfois vitaux en matière de continuité d'activité ou de découplage de filiale, et d'assumer les responsabilités légales inhérentes à la situation.
- **Protéger la réputation de l'organisation et la confiance de l'écosystème.** Le Conseil agit comme pilote de la communication de haut niveau vis-à-vis des marchés financiers, des régulateurs (tels que la CNIL ou l'ANSSI) et des actionnaires. Il se porte garant d'une transparence proactive, évitant que le silence ne soit jugé plus sévèrement que la vulnérabilité elle-même.

2.2.3 PILOTAGE PAR LES MÉTRIQUES - VECTEUR #3

En matière de mesure de la performance de la sécurité numérique, les conseils d'administration sont attendus pour :

- **Évaluer l'alignement entre ressources allouées et couverture réelle des risques.** Les administrateurs doivent veiller à ce que les indicateurs stratégiques d'exposition aux risques réels restent alignés avec les seuils de tolérance en vigueur. Le cas échéant, le Conseil doit pouvoir s'appuyer sur des benchmark sectoriels (données assureurs, ou audits indépendants), pour évaluer l'enveloppe, la maturité et le retour sur investissement de la sécurité numérique.
- **Sécuriser les transformations majeures.** Les Conseils doivent pouvoir demander un suivi spécifique pour tout projet structurant (M&A, nouvelles filiales, réorganisation majeure, plan de transformation/d'intégration de nouvelles technologies comme l'IA) afin de prévenir de nouvelles vulnérabilités systémiques.

Rôles d'approbateur (*accountable*) du conseil d'administration par grands vecteurs de la gouvernance de la sécurité numérique							
Vecteur #1 *Politique de la sécurité numérique*	Définir l'ambition de la gouvernance	Comprendre son activité numérique	Connaître son seuil d'acceptation des risques	Apprécier les risques numériques	Définir sa stratégie et sa valorisation	Définir des polices d'assurance adaptées	Placer l'humain au centre du jeu
Vecteur #2 *Application de la politique au quotidien*	Qualifier ses services numériques critiques	Bâtir sa protection	Orienter sa défense et anticiper sa réaction	Faire preuve de résilience en cas de cyberattaque	Suivi de la conformité réglementaire en interne	Entretien de l'hygiène numérique et des bonnes pratiques	
Vecteur #3 *Pilotage, suivi et communication*	Mesure de la performance	Analyse de la performance	Communication du suivi et de la performance				

Figure 11 : Synthèse - Cartographie des responsabilités du conseil d'administration

AVIS D'EXPERT

Gouvernance de la sécurité numérique : l'exigence du réalisme et de l'impulsion stratégique du conseil d'administration

Ancré dans les fondements de la loi de 1966, le rôle du conseil d'administration (CA) est déterminant pour la performance et la création de valeur des organisations, qu'elles soient cotées ou non. En tant qu'organe non-exécutif, sa mission première consiste à identifier les risques critiques, définir les orientations stratégiques et contrôler leur mise en œuvre effective par la direction générale.

Toutefois, le caractère intermittent du Conseil crée *de facto* une asymétrie d'information structurelle avec l'exécutif. Pour pallier ce déficit et garantir des décisions les plus éclairées possibles, les administrateurs doivent aller proactivement au-delà de la seule lecture des documents fournis par la direction. Ils doivent fournir un véritable effort de compréhension et d'investigation personnelle et bénéficier, en particulier, d'un accès direct aux directeurs clés, notamment au CIO Groupe, afin d'obtenir des réponses claires à des questions simples, avec des indicateurs d'activités adaptés aux responsabilités des administrateurs.

Si la prise de conscience de la menace numérique est réelle depuis les attaques majeures à l'encontre de Saint-Gobain en 2017, le niveau de dialogue et de coopération entre le Conseil, la direction générale et la fonction numérique devrait considérablement monter en intensité. Le Conseil doit en ce sens pleinement assurer son rôle d'impulsion stratégique, et ne pas se contenter de valider des orientations souvent préétablies, *de facto*, par le comité exécutif. L'objectif stratégique, en matière de gouvernance de la sécurité numérique comme ailleurs, est de ne plus subir la crise, mais de la devancer. Cela exige de fluidifier la remontée d'information, de s'assurer de la cohérence des documents de pilotage (de la cartographie des risques aux plans de continuité et de reprise d'activité) et de réaliser des exercices de crise conjoints, rassemblant Conseil, Direction et fonction numérique.

Concrètement, il relève de la responsabilité des administrateurs d'interroger à l'aide de questions précises l'importance, la pertinence et la fréquence accordée aux enjeux de sécurité numérique au sein du Comex : quelle place ce sujet occupe-t-il dans l'ordre du jour ? Quel temps de parole est prévu ? Sous quel angle la présentation est-elle réalisée ? Quels indicateurs sont revus ? Quelles questions ont été posées ? Combien de fois par an le sujet est-il abordé ? Autant d'éléments qui doivent être mis à l'épreuve en interne, sous l'impulsion du Président du Conseil, et le plus possible étalonnés par rapport aux pratiques du secteur.

Alors que les organisations françaises sont aujourd'hui, même malgré elles, traversées par de fortes attentes sociales et des enjeux géopolitiques des plus globaux, les conseils d'cdministration ont un rôle important à jouer pour définir des politiques numériques réalistes et créatrices de valeur. C'est là un enjeu de puissance et de pouvoir pour l'organisation, de pérennité et d'influence, qui dépasse la seule analyse financière ou réglementaire pour toucher

au cœur de l'acceptation des risques. Pour les administrateurs, la question fondamentale reste celle de la réalisation du but social de l'organisation par l'atteinte de sa proposition de valeur, critère principal de la criticité.

Pour maintenir ce cap dans un monde complexe, le Conseil doit intégrer une culture d'intelligence économique et de réalisme géopolitique. À ce titre, les comités de nomination devraient désormais veiller à intégrer de véritables compétences cyber au sein des matrices de compétences des administrateurs. C'est à ce prix, et par la qualité du travail humain entre la direction générale, le Conseil et la fonction numérique, que la gouvernance de la sécurité numérique pourra discerner les champs de force à l'œuvre et naviguer avec clairvoyance dans les rapports contradictoires qui s'y exercent.

Caroline Ruellan, Présidente, Cercle des Administrateurs

2.3 IMPLICATIONS POUR LA DIRECTION GÉNÉRALE / COMEX : PROPOSITION, CADRAGE ET IMPULSION DE MISE EN ŒUVRE

Pour que la sécurité numérique devienne un véritable levier de performance et de compétitivité, la direction générale a un rôle fondamental de proposition, de cadrage et d'impulsion à exercer.

Selon les modèles de gouvernance, la direction générale assume le rôle de garante exécutive (*Responsible*) ou de responsable (*Accountable*) rendant des comptes au Conseil. Il lui appartient dans tous les cas d'insuffler la dynamique nécessaire pour traduire les orientations stratégiques en réalité opérationnelle et aligner les ambitions de sécurisation avec les impératifs métiers.

Un des principaux défis est de faire valoir une vision pragmatique et fédératrice, dépassant le simple cadre des bonnes pratiques. En effet, avec l'entrée en vigueur de la directive européenne NIS2 (octobre 2024), la responsabilité légale du dirigeant exécutif [18] est directement engagée quant à la mise en œuvre effective de la gouvernance et des mesures de gestion des risques associées (Art. 20.1). Les sanctions peuvent aller jusqu'à la suspension temporaire des fonctions dirigeantes, en cas de manquements graves et répétés. L'article 20.2 de la directive NIS2 concerne également les comités exécutifs. Il oblige les Comex à suivre une formation leur permettant d'acquérir les compétences suffisantes pour identifier les risques et évaluer les pratiques de gestion des risques de sécurité numérique. Cet article devient alors une condition *sine qua non* de l'exercice de leur responsabilité, accompagnée de l'obligation d'impulser des programmes de sensibilisation réguliers pour l'ensemble des collaborateurs.

Le *vade-mecum* ci-après se veut une proposition de synthèse des responsabilités attendues de la direction générale en matière de sécurité numérique.

[18] Plus de détails fournis par le référentiel ReCyf et MonEspaceNIS2 de l'ANSSI

2.3.1 CONTRIBUTION À LA CONSTRUCTION DE LA PSN - VECTEUR #1

En matière de structuration de la stratégie et d'allocation des moyens, la direction générale est tout particulièrement attendue pour :

- **Mettre en place et animer un cadre de gouvernance au service de la résilience**. La direction générale doit instituer un comité stratégique de la sécurité numérique réunissant, *a minima*, un membre de chacune des « trois lignes de maîtrise » (management opérationnel, fonctions support/risques et audit interne). Un représentant de la direction générale peut être désigné pour assurer en particulier le *sponsoring* de cette gouvernance. En matière de gestion de la performance, ce membre du comité exécutif pourra :
  - Superviser le programme de sécurité numérique dans son ensemble, grâce au travail d'un second comité, le comité décisionnel chargé de la « vision portefeuille » ;
  - Déléguer le pilotage détaillé du programme de sécurité numérique à un troisième comité, le comité opérationnel chargé de la « vision projets ».
- **Aligner orientations stratégiques, feuille de route et investissements**. Il appartient à la direction générale d'interroger et d'approuver la Politique de Sécurité Numérique (PSN), dont elle délègue la rédaction. Elle s'assure que cette stratégie se traduit systématiquement par des budgets et des ressources capacitaires adaptées à sa mise en œuvre dans la durée.
- **Traduire l'appétence au risque en critères d'arbitrage**. La direction générale doit définir un seuil d'acceptation des risques internes et exiger sa traduction en éléments tangibles, afin de prioriser les investissements. Cela passe notamment par l'action :
  - D'évaluer les risques liés aux manquements « d'hygiène numérique » ;
  - D'évaluer les risques de non-conformité et la définition d'objectifs chiffrés et temporalisés de mise en conformité, éventuellement à l'aide d'une charte ;
  - D'évaluer les vulnérabilités des services numériques (systèmes ou actifs) les plus critiques de l'organisation, en exigeant pour ces derniers une véritable démarche d'homologation de sécurité ;
  - D'évaluer le rapport entre le coût de la couverture et les impacts chiffrés des principaux sinistres scénarisés et retenus.
- **Arbitrer la réduction des risques résiduels et définir une politique de transfert par assurance**. Après avoir validé le plan de réduction des risques, la direction générale doit statuer sur le risque résiduel. Il s'agit d'identifier et de souscrire la couverture d'assurance la plus adéquate face aux risques directs, indirects et induits, en couvrant impérativement les quatre piliers de l'assurance en matière de sécurité numérique : la prévention, l'assistance, les opérations et la responsabilité.
- **Garantir, pour les différents types de risques, l'autonomie stratégique par la maîtrise des dépendances**. Il s'agit d'assumer en matière de sécurité numérique une interdépendance choisie à l'égard des tiers, en maintenant un degré de maîtrise décisionnelle et capacitaire suffisants. Le Comex doit exercer une forte vigilance systémique couvrant les sous-jacents géopolitiques, économiques, juridiques et technologiques, afin de prévenir l'exploitation abusive de situations

asymétriques. En tant que garant de la liberté de choix des objectifs et de l'exercice des moyens, le comité exécutif s'assure d'une réelle capacité de choix (*multi-sourcing*) et d'un contrôle strict sur les leviers contractuels et opérationnels : gouvernance de la donnée, garanties de continuité en cas de ruptures diplomatiques, et clauses de réversibilité robustes permettant la substitution ou l'internalisation partielle des activités, y compris en mode dégradé.

- **Valoriser la démarche et les investissements**. Il revient enfin au Comex de définir une stratégie de valorisation de ces efforts, en démontrant en interne comme en externe que la sécurité numérique est un avantage concurrentiel et un levier de confiance pour tout l'écosystème.

2.3.2 MISE EN APPLICATION AU QUOTIDIEN - VECTEUR #2

Au quotidien, et tout particulièrement en situation de crise, la direction générale doit maintenir une posture de supervision active et de prise de décision rapide, dans le but de :

- **Sanctuariser l'hygiène numérique par l'évaluation continue.** Il revient au Comex de s'assurer de l'efficacité réelle des mesures de sécurité numérique mises en place. Il est en capacité de mandater des tiers de confiance indépendants pour la conduite d'audits de sécurité (techniques, organisationnels, etc.) et d'exiger le suivi des plans de remédiation qui en découlent.
- **Superviser la trajectoire de conformité réglementaire.** Le Comex doit pouvoir s'assurer que l'organisation reste alignée avec ses obligations légales, sans pour autant s'immiscer dans le suivi technique quotidien. Il est en mesure de demander des *reportings* réguliers sur le dispositif de mise en conformité par la fonction numérique, et arbitre les trajectoires de remédiation avant toute communication externe.
- **Garantir la résilience et piloter la gestion de crise stratégique.** En cas d'incident majeur de sécurité numérique, le Comex dirige et assume la responsabilité de la survie de l'organisation. Cela implique d'exécuter les actions suivantes :
  - Diriger la cellule de crise stratégique (en tant que *Responsible*), tout en déléguant et en sponsorisant l'action de la cellule opérationnelle ;
  - Orchestrer et valider la communication de crise auprès des collaborateurs, clients, partenaires, médias, afin d'endiguer les effets collatéraux et de préserver la réputation de l'organisation ;
  - Garantir l'effectivité de la continuité d'activité. « En temps de crise », cela passe par le déploiement des Plans de Continuité d'Activité (PCA) et des Plans de Reprise d'Activité (PRA) et, « en temps calme » par l'exigence d'une planification d'exercices d'entraînement réguliers et collectifs.
  - Maintenir la réactivité réglementaire et assurantielle par l'entretien des relations avec l'assureur (activation immédiate des garanties), et la vérification du bon respect des obligations de notification aux autorités compétentes (notamment dans les délais imposés par la directive NIS2).

2.3.3 PILOTAGE PAR LES MÉTRIQUES - VECTEUR #3

Pour éclairer ses prises de décision, justifier l'allocation des ressources et rendre des comptes au Conseil, la direction générale ne peut se contenter d'évaluations subjectives et doit pouvoir :

- **Intégrer la mesure de la performance face à la menace.** Le Comex doit s'assurer de l'existence d'un dispositif de suivi des risques et intégrer systématiquement ces analyses dans les processus stratégiques de l'organisation. Il attend de la fonction numérique la définition d'outils de pilotage permettant :
  - D'évaluer le niveau et l'évolution de la menace (tactiques, techniques, procédures) pesant sur les différentes activités de l'entreprise et les actifs visés ;
  - D'évaluer l'état de maturité de la sécurité numérique par catégorie d'action (identification, protection, détection, réponse, remédiation) ;
  - D'évaluer la fenêtre critique de vulnérabilité (ratio surface d'exposition/taux de couverture, incluant les risques non-anticipés) ;
  - D'évaluer l'avancement pluriannuel des objectifs.
- **Mesurer l'engagement managérial et la culture de sécurité.** Le risque humain étant prépondérant, le Comex doit évaluer la performance de l'organisation dans l'acculturation de ses collaborateurs. Les métriques exigées doivent refléter :
  - L'intégration d'objectifs de cybersécurité (et d'éventuelles incitations financières associées) dans l'évaluation des managers, ainsi que la bonne intégration de cette dimension dans les délégations de pouvoir ;
  - L'efficacité des actions de sensibilisation et de formation : pourcentage de collaborateurs formés ou testés, niveau de maturité par profils (notamment selon la criticité des rôles), et régularité de la communication interne.
- **Analyser l'efficacité opérationnelle et la maîtrise des vulnérabilités.** La direction générale commandite un rapport global régulier analysant l'application effective de la Politique de Sécurité Numérique (PSN) et les écarts avec la gouvernance cible. Elle doit y retrouver des indicateurs consolidés tels que :
  - Le niveau d'intégration de la sécurité dès la conception (*Security by design*) dans les nouveaux projets ;
  - L'efficacité de la détection et de la correction des failles : plutôt que des volumes bruts, le Comex suit des ratios de performance (taux de vulnérabilités critiques corrigées dans le trimestre, reste à faire, volume de failles ramené à la taille du parc) ;
  - Le niveau de conformité du maintien en conditions de sécurité du système d'information (taux de *patch management*).
- **Consolider la prise de décision via un tableau de bord stratégique.** Pour asseoir sa responsabilité exécutive, le Comex doit pouvoir disposer d'un tableau de bord de synthèse, avec des métriques et un langage commun avec la fonction numérique. Ce document, qui a vocation à être communiqué au conseil d'administration, consolide les données qualitatives et quantitatives, met en perspective

l'actualité de la menace avec l'analyse des risques de l'entreprise, et évalue le rapport coût-efficacité des investissements réalisés.

Rôles d'approbateur (*accountable*) de la direction générale par grands vecteurs de la gouvernance de la sécurité numérique							
Vecteur #1 *Politique de la sécurité numérique*	Définir l'ambition de la gouvernance	Comprendre son activité numérique	Connaître son seuil d'acceptation des risques	Apprécier les risques numériques	Définir sa stratégie et sa valorisation	Définir des polices d'assurance adaptées	Placer l'humain au centre du jeu
Vecteur #2 *Application de la politique au quotidien*	Qualifier ses services numériques critiques	Bâtir sa protection	Orienter sa défense et anticiper sa réaction	Faire preuve de résilience en cas de cyberattaque	Suivi de la conformité réglementaire en interne	Entretien de l'hygiène numérique et des bonnes pratiques	
Vecteur #3 *Pilotage, suivi et communication*	Mesure de la performance	Analyse de la performance	Communication du suivi et de la performance				

Figure 12 : Synthèse - Cartographie des responsabilités de la direction générale

3 QUATRE ARCHÉTYPES ORGANISATIONNELS DE SÉCURITÉ NUMÉRIQUE POUR UNE GOUVERNANCE SUR-MESURE

3.1 VARIABLES D'ARBITRAGE CLÉS DE LA GOUVERNANCE DE LA SÉCURITÉ NUMÉRIQUE

Après avoir structuré le cadre de gouvernance de la sécurité numérique sur ses trois vecteurs (politique de sécurité numérique, application au quotidien, pilotage par les métriques), la déclinaison organisationnelle constitue une étape essentielle pour le déploiement effectif de la gouvernance.

Pour calibrer le modèle de gouvernance le plus propre au contexte de son organisation, plusieurs arbitrages structurants doivent être tranchés. Ces arbitrages impliquent une démarche globale de l'organisation autour de quelques variables clés. En effet, différentes questions se posent dès la phase de définition de l'appétence au risque et de sa qualification, les problématiques de création de valeur, de portage de la responsabilité et de rattachement organisationnel :

- **Quelle approche privilégier pour maximiser la contribution de la sécurité numérique** au modèle d'affaires de l'organisation ?
- **Quelle implication demander au conseil d'administration, au comité exécutif,** à la fonction numérique, aux métiers, aux départements des risques et de la sûreté, à l'audit interne ou externe ?
- **Comment échelonner dans le temps la construction, la comparaison inter-filiales et le pilotage global des moyens de sécurité numérique**, tout en assumant les tensions locales entre l'harmonisation du niveau de maturité et de sécurité et la diversité des actifs et architectures ? Comment transmettre ou déléguer aux métiers des responsabilités "*Accountability*", appartenant au conseil d'administration ou à la direction générale, qui les engagent même pénalement, sans diluer ni le contrôle, ni la transversalité, ni l'autonomie locale ?
- **Comment équilibrer la structuration interne et son pilotage avec les différentes expositions externes** à la conformité et aux instances de régulation, au contexte international, et vis-à-vis des fournisseurs et de leurs chaînes de sous-traitance ?

Au cours des sessions du groupe de travail du Cigref, ces interrogations se sont cristallisées autour de quatre variables clés que sont :

1. **Le positionnement stratégique**
2. **Le modèle organisationnel**
3. **L'intégration opérationnelle**
4. **Les expositions externes.**

Pour décliner la gouvernance de la sécurité numérique sur le plan organisationnel, chacune de ces 4 variables clés a été plus finement détaillée en critères d'appréciation. Rattachés aux 4 variables clé, ce sont donc 11 critères au total qui ont été identifiés par les participants au groupe de travail, afin de permettre à chaque organisation de calibrer un modèle de gouvernance le plus efficient et sur-mesure possible.

3.1.1 PREMIÈRE VARIABLE : LE POSITIONNEMENT STRATÉGIQUE

La première variable clé d'arbitrage, le positionnement stratégique, concerne la place du numérique, et donc de la sécurité numérique, dans la chaîne de valeur de l'organisation, avec deux deux questions fondamentales qui se posent :

- **L'exposition aux menaces stratégiques**. Dans l'esprit de la directive européenne NIS 2 et de sa transposition prochaine en droit français, une démarcation claire s'opère entre les risques cybercriminels de masse et les menaces stratégiques ciblées. Cette approche consacre un principe de proportionnalité, actant qu'un Opérateur d'Importance Vitale (OIV), une Entité Essentielle (EE) ou Importante (EI) ne se sécurise pas de la même manière qu'une PME.

- **La contribution stratégique de la fonction numérique au modèle d'affaires en tant que fonction support** implique que la sécurité numérique aura plutôt tendance à adopter une posture experte et conforme. Dans le cas contraire, si le numérique ou la sécurité au sens large sont au cœur du modèle d'affaires, la sécurité numérique devrait être soit mobilisée comme un facilitateur d'activité, soit intégrée nativement et systématiquement comme un actif stratégique.

Ces différences fondamentales déplacent le curseur sécuritaire de la compétence technique pure vers une intégration plus récurrente dans les processus métiers. Ce mouvement de balancier est souvent traduit par un transfert des activités de la fonction numérique des couches infra vers les couches applicatives.

3.1.2 DEUXIÈME VARIABLE : LE MODÈLE ORGANISATIONNEL

La seconde variable clé d'arbitrage concerne l'architecture du pouvoir décisionnel, qui repose sur l'équilibre entre centralisation et décentralisation à trois niveaux différents :

- **Centralisation (ou décentralisation) de l'action pour la fonction numérique**. Le modèle de services partagés (ou *Shared Services*) au niveau Groupe peut en ce sens être un moyen de fixer une base minimale de cohérence globale et d'accorder pour le reste une autonomie complète aux filiales.

- **Centralisation (ou décentralisation) des budgets**. Outre la sélection des projets, cet enjeu concerne la taille des équipes dédiées à la sécurité numérique et les compétences à rechercher à l'interne ou à externaliser.

- **Arbitrage critique en faveur de la continuité d'activité en mode dégradé (ou l'interruption de l'activité au profit de la qualité de service)**. Deux environnements organisationnels antagonistes peuvent illustrer ce besoin d'arbitrage : dans un contexte sanitaire par exemple, la continuité de service numérique peut s'avérer vitale et ne peut être interrompue sans mettre en péril la mission fondamentale de l'institution, tandis que dans un contexte industriel, la qualité des biens proposés peut, à l'inverse, être jugée vitale, en raison d'éventuels incidents et rappels en production que la qualité dégradée pourrait susciter. La construction du modèle de gouvernance de son organisation doit pouvoir, à ce titre, clarifier le lien et le transfert de pouvoir qui peut être réalisé entre ceux qui détiennent les budgets, ceux qui portent le risque opérationnel et ceux qui peuvent porter la responsabilité légale.

3.1.3 TROISIÈME VARIABLE : L'INTÉGRATION OPÉRATIONNELLE

La troisième variable clé d'arbitrage interroge la capacité de l'organisation à harmoniser ses pratiques sans étouffer les spécificités locales, selon au moins trois angles :

- **L'harmonisation (ou la diversité) des niveaux de sécurité**. L'harmonisation globale risque d'aligner la performance sur le maillon le plus faible, tandis qu'une diversification excessive complexifie le maintien en condition opérationnelle et en condition de sécurité.
- **La mutualisation des actifs de sécurité (ou leur caractère distribué à travers l'organisation)**. La maîtrise des coûts par mutualisation de certains actifs clés (SOC ou CSIRT par exemple) peut être un levier opérationnel pour permettre à toutes les filiales d'avoir un socle de maturité commun pour la sécurité numérique.
- **Le silotage (ou la transversalité) de la sécurité numérique**. Avec un silotage très fort, le risque est de créer par la sécurité numérique une « seconde DSI » qui agirait soit comme une autre fonction support, soit comme un gendarme bloquant, au lieu de définir un contrat de service clair et global (conseil, faiseur, contrôleur). À l'opposé, la transversalité complète de la sécurité numérique pourrait diluer son impact en la cantonnant à un rôle de conseiller en processus de gouvernance.

3.1.4 QUATRIÈME VARIABLE : LES EXPOSITIONS EXTERNES

Quatrième et dernière variable d'arbitrage clé du modèle de gouvernance, les expositions externes doivent bien sûr s'adapter à l'écosystème dans lequel évolue l'organisation, sous au moins trois rapports :

- **L'intensité de l'exposition au contexte international**. En sous-jacent de toute stratégie organisationnelle de « *follow the sun* », ou commerciale de conquête d'un marché, s'ajoute la question de la diversité quantitative des zones géographiques d'implantation de l'organisation et la volatilité géopolitique variable selon ces zones.
- **L'intensité de l'exposition à la régulation (pas seulement numérique)**. Que ce soit sous l'angle sectoriel ou géographique, la pression réglementaire joue un rôle déterminant dans les arbitrages à réaliser en matière de gouvernance. La structure capitalistique de l'organisation et le degré de sensibilité des informations qu'elle détient ou opère, ont un rôle substantiellement différent en fonction des régulations auxquelles l'organisation est exposée.
- **L'exposition aux fournisseurs**. La dépendance aux fournisseurs (de solutions numériques ou intégrant une composante numérique dans leurs offres) pose notamment la question de la « taille critique » : l'organisation a-t-elle la masse critique pour internaliser une partie des compétences pointues en sécurité numérique ? Doit-elle par ailleurs se contenter de piloter ponctuellement des fournisseurs et prestataires sans contrôle effectif ? Ce positionnement détermine la capacité de sécurisation de sa chaîne de valeur étendue, au-delà des audits internes.

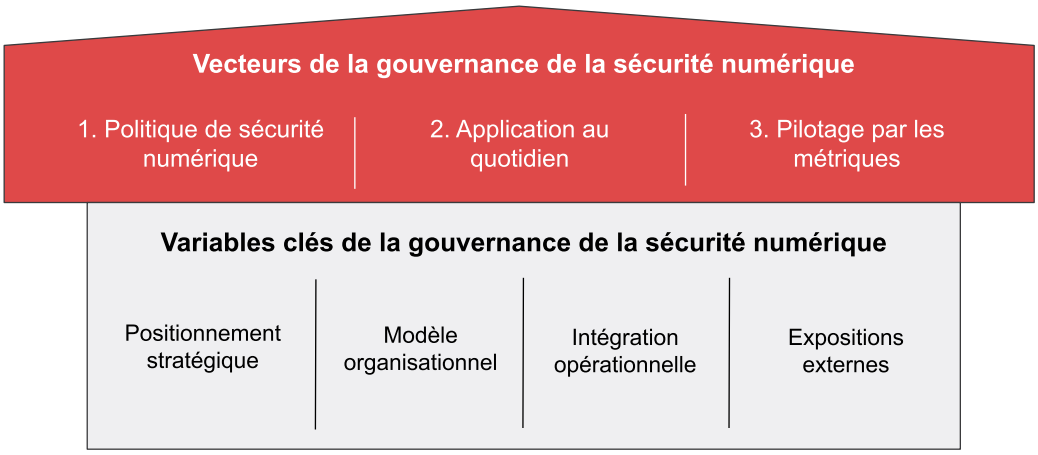


Figure 13 : Synthèse - 4 variables clés d'arbitrage pour décliner sa gouvernance de la sécurité numérique

3.1.5 DÉCLINAISON DES VARIABLES CLÉS EN CRITÈRES D'APPRÉCIATION

Les différentes problématiques décrites selon ces 4 variables clés d'arbitrage ont permis au groupe d'établir une matrice de 11 critères d'appréciation pour aider les décideurs du numérique à déterminer le modèle de sécurité le plus efficient et le plus adapté à leur organisation. Les critères d'appréciation, selon chaque variable sont les suivant :

Positionnement stratégique

- Critère d'appréciation #0 | Exposition aux menaces : stratégiques VS cybercriminelles
- Critère d'appréciation #1 | La fonction numérique : support VS cœur du métier

Modèle organisationnel

- Critère d'appréciation #2 | Décisions : centralisées VS décentralisées
- Critère d'appréciation #3 | Budgets : centralisés VS décentralisés
- Critère d'appréciation #4 | Priorité accordée à : la continuité d'activité VS la qualité de service

Intégration opérationnelle

- Critère d'appréciation #5 |Niveaux de sécurité : homogènes VS hétérogènes à travers l'organisation
- Critère d'appréciation #6 | Actifs de sécurité : mutualisés VS distribués
- Critère d'appréciation #7 | Enjeux de sécurité numérique distincts par : silos VS transversaux

Expositions externes

- Critère d'appréciation #8 | Exposition au contexte international : faible VS forte
- Critère d'appréciation #9 | Exposition aux régulations : faible VS forte
- Critère d'appréciation #10 | Exposition aux fournisseurs externes : faible VS forte

3.2 PRINCIPAUX ARCHÉTYPES DE GOUVERNANCE DE LA SÉCURITÉ NUMÉRIQUE

L'élaboration de plusieurs scénarios de gouvernance par le groupe de travail a permis d'établir une cartographie de l'état de l'art des modèles d'organisation de la sécurité numérique. Les archétypes de gouvernance ont pour vocation de servir à la création de valeur par la sécurité numérique, et à sa mise en visibilité. Ils constituent pour chaque organisation une grille d'analyse de ses forces et faiblesses actuelles, facilitant l'anticipation d'évolutions prospectives nécessaires à la résilience de sa gouvernance.

Chaque archétype est donc décliné en une fiche présentant :

- Les 11 critères d'appréciation de gouvernance associés,
- Une proposition de valeur phare,
- Un rattachement organisationnel privilégié,
- Une analyse du positionnement stratégique.

3.2.1 ARCHÉTYPE 1 - « EXPERT ET PARTENAIRE »

3.2.1.1 Proposition de valeur

L'archétype « Expert et partenaire » répond aux besoins d'innovation technologique par des cas d'usage métiers. Sa valeur ajoutée est centrée sur l'expertise technique et le partenariat, au service de la réussite des objectifs métiers. Il privilégie la fluidité de l'expérience utilisateur et s'appuie sur une forte agilité dans l'intégration sécurisée des solutions du marché.

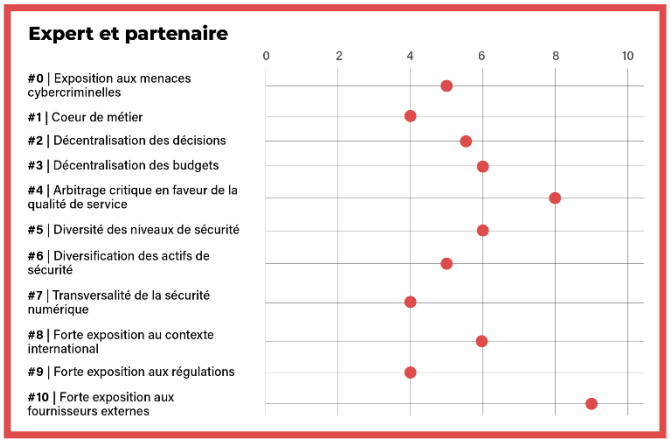


Figure 14 : Archétype 1 « Expert et partenaire »

Le rattachement organisationnel privilégié pour cet archétype de gouvernance situe la sécurité numérique auprès de la fonction numérique (CIO / CTO), en collaboration étroite avec le département des risques qui agit comme une seconde ligne de défense pour objectiver les arbitrages et éviter la position de juge et partie.

3.2.1.2 Analyse du positionnement stratégique

Optimiser son modèle de gouvernance	**Expert et partenaire** Proposition de valeur centrée autour des besoins métiers et de l'innovation technologique, avec une valeur ajoutée centrée sur l'expertise technique et le partenariat au service de la réussite des objectifs métiers. Habituellement rattaché à la fonction numérique, en collaboration avec le département risques.
Points de différenciation	• Crédibilité des décisions techniques prises • Fiabilité des solutions déployées • Agilité face aux demandes d'évolutions technologiques
Points de vigilance	• Conflit d'intérêt technico-commercial • Posture réactive de prestataire interne • Déploiement transversal des solutions
Facteurs clés de succès	• Anticiper la valeur des développements technologiques pour les métiers, par une démarche de veille active et un outillage en R&D. • Être force de proposition dans le choix des architectures sécurisées, en créant les conditions d'adhésion, de distribution et d'innovation par les métiers (e.g, la capacité à transformer le "Shadow IT" en "IA citoyenne"). • Traduire dans un langage COMEX les enjeux de sécurité numérique en impacts business, financiers ou réputationnels pour mobiliser les métiers et co-piloter les projets par les risques.

3.2.2 ARCHÉTYPE 2 - « CONFORMITÉ ET AFFAIRES PUBLIQUES »

3.2.2.1 Proposition de valeur

L'archétype « Conformité et affaires publiques » est centré autour de la gestion des risques et la maîtrise de la réglementation. Sa valeur ajoutée réside dans la gestion par les risques, le contrôle et la surveillance de la « capacité légale à exercer », au profit de son organisation. Il est caractérisé par une priorité accordée à la recherche d'une sécurisation collective, à la fédération d'acteurs autour d'exercices communs et se trouve souvent associé aux activités des Affaires Publiques au sein des processus législatifs et normatifs, de leur élaboration à leur déploiement.

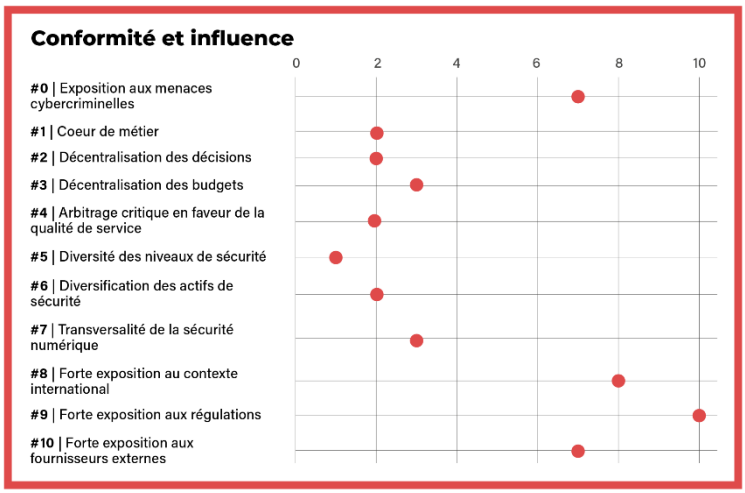


Figure 15 : Archétype 2 « Conformité et affaires publiques »

Le rattachement organisationnel privilégié pour cet archétype de gouvernance situe la sécurité numérique auprès de la Direction des Risques, du Secrétariat Général, de la Direction de la Conformité ou de la Direction Financière. Si la maturité et les ressources le permettent, un dédoublement des compétences de sécurité numérique peut avoir lieu au sein de la fonction numérique (CIO) qui maintient un rôle décisionnaire, notamment en matière financière et opérationnelle.

3.2.2.2 Analyse du positionnement stratégique

Optimiser son modèle de gouvernance	**Conformité et affaires publiques** Proposition de valeur centrée autour de la gestion des risques, avec une valeur ajoutée centrée sur une recherche de conformité maximale et la capacité à contribuer directement aux processus législatifs et normatifs associés, dès leur élaboration. Habituellement rattaché aux départements des Risques et/ou de la Conformité, en collaboration avec la fonction numérique.
Points de différenciation	• Capacité à transformer la contrainte réglementaire en barrière à l'entrée pour les concurrents • Connaissance parfaite du patrimoine informationnel et contrôle rigoureux • Développement de partenariats, implication législative, par une stratégie robuste d'Affaires Publiques
Points de vigilance	• Lourdeur procédurale allongeant les délais de mise sur marché, décourageant les innovations métiers • Illusion d'une sécurisation optimale par les seuls efforts de mise en conformité et de création de règles • Inflation des budgets dédiés aux audits et au reporting plutôt qu'à la scénarisation d'attaques personnalisées.
Facteurs clés de succès	• Industrialiser la conformité par un recours fréquent à l'automatisation des contrôles, du reporting et de la veille réglementaire • Démontrer aux métiers l'enjeu réel que représentent les standards de sécurité élevés en matière de responsabilité pénale et d'image de marque • Transformer les certifications techniques obtenues en label de confiance et levier de partenariats

3.2.3 ARCHÉTYPE 3 - « PLATEFORMISATION ET GOUVERNANCE »

3.2.3.1 Proposition de valeur

L'archétype « Plateformisation et gouvernance » tire sa valeur de sa capacité à aligner la sécurité sur les enjeux métiers, via une approche de « contrat de service » interne large et performant. Il se caractérise par une volonté de faire de la sécurité numérique une filière distribuée transversalement au sein des directions métiers, dans le but de faire de la sécurité numérique un « facilitateur business ».

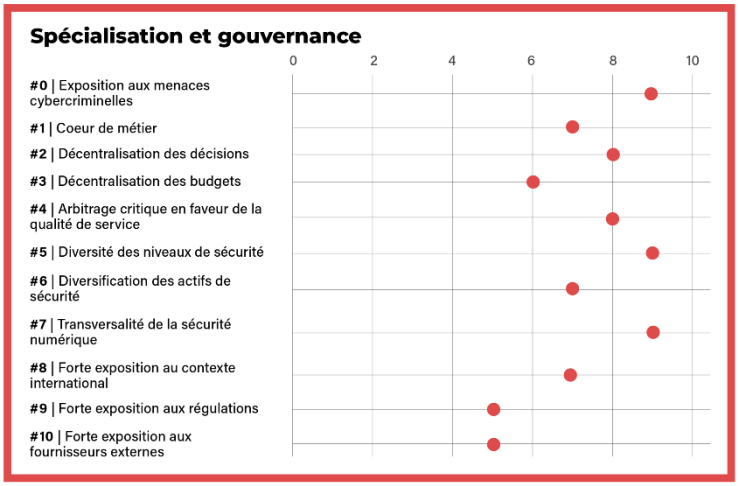


Figure 16 : Archétype 3 « Plateformisation et gouvernance »

Le rattachement organisationnel privilégié pour cet archétype de gouvernance positionne la sécurité numérique en lien direct avec la direction générale, et de manière distincte de l'implication de la fonction numérique au comité exécutif. Le positionnement matriciel de la sécurité numérique au cœur du modèle d'affaires est couplé à un rôle de partage et d'orchestration des responsabilités avec les métiers.

3.2.3.2 Analyse du positionnement stratégique

Optimiser son modèle de gouvernance	**Plateformisation et gouvernance** Proposition de valeur centrée autour d'une offre de service interne large et performante de sécurité numérique, associée à la définition et au suivi d'un cadre de gouvernance et de partage des responsabilités avec les métiers. Habituellement rattaché directement à l'exécutif, avec une priorité donnée à l'autonomisation de la sécurité numérique pour assumer un rôle de catalyseur et facilitateur d'activité.
Points de différenciation	• Proposition d'un catalogue de services mutualisés, avec des engagements de service clairs pour les métiers • Combinaison d'expertise technique et de compétences de gestion dans les équipes (projet, communication, finance) • Distribution de la sécurité dans les coeur de métiers, créant un maillage opérationnel de Cyber Champions proactifs
Points de vigilance	• Complexité matricielle dans la décentralisation réelle des responsabilités • Coût total de maintien d'un panel d'offres de service internes de haute qualité • Exposition politique de la sécurité numérique avec d'éventuelles incidences sur ses arbitrages techniques
Facteurs clés de succès	• Définir sans ambiguïté les responsabilités des différentes entités, pour faire de la fonction numérique et de sa sécurité un levier de résilience et de compétitivité au coeur du modèle d'affaire de l'organisation • Incarner la sécurité numérique au-delà de l'expertise technique, à partir de savoirs-être permettant influence, diplomatie et valorisation financière de la sécurité numérique • Mettre en place des indicateurs de performance et de risque orientés business, permettant de justifier le rendement des services internes

3.2.4 ARCHÉTYPE 4 - « SÉCURITÉ INTÉGRÉE »

3.2.4.1 Proposition de valeur

L'archétype « Sécurité intégrée » tire sa valeur de sa capacité à gérer le continuum de la menace de manière holistique. Sa valeur ajoutée réside dans une protection unifiée couvrant à la fois les actifs physiques et numériques et garantissant la sûreté opérationnelle globale. Il est caractérisé par une approche décloisonnée visant à contrer les menaces dans toutes leurs formes, physiques et numériques (espionnage, sabotage, terrorisme), par une surveillance et une réponse unifiée.

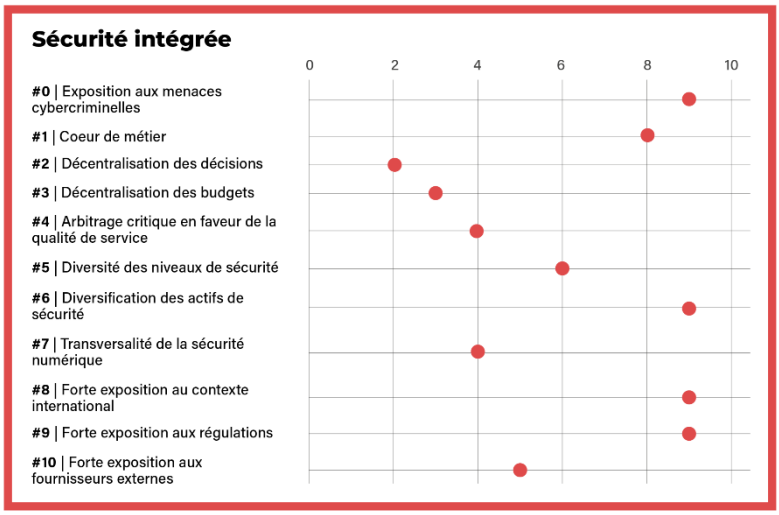


Figure 17 : Archétype 4 « Sécurité intégrée »

Le rattachement organisationnel privilégié pour cet archétype de gouvernance situe la sécurité numérique au sein d'une Direction de la Sûreté globale (CSO - Chief Security Officer) ou du Secrétariat Général. La priorité est donnée à la convergence des opérations : l'analyse de risque, la surveillance et la gestion de crise sont pilotées conjointement. La gestion dépend d'une vision régalienne où la donnée est un actif critique à protéger au même titre que les infrastructures industrielles ou les collaborateurs.

3.2.4.2 Analyse du positionnement stratégique

Optimiser son modèle de gouvernance	**Sécurité intégrée** Proposition de valeur centrée autour de la gestion intégrée de la sécurité, avec portage la responsabilité de la sécurité opérationnelle globale des actifs physiques et numériques. Habituellement rattaché au département de la sécurité globale (CSO), avec une priorité donnée à la gestion du continuum de la menace hybride (physique et numérique) et des opérations (analyse des risques et gestion de crise)
Points de différenciation	• Vision à 360° de la sécurité numérique permettant de détecter les menaces hybrides (physique-cyber) • Culture opérationnelle du "Command & Control" favorisant la réactivité et la discipline en cas de crise • Mutualisation des outils de surveillance et des renseignements sur le continuum de la menace
Points de vigilance	• Fluidité du dialogue et culture commune entre la fonction numérique et la sûreté en matière de sécurité • Sous-estimation des spécificités techniques de la sécurité numérique par l'approche de protection globale • Risque de "Shadow IT" si les mesures de sécurité sont perçues comme des freins trop lourds par les métiers
Facteurs clés de succès	• Développer une culture de sécurité commune où chaque incident est analysé sous le double prisme physique et logique • Mettre en place une gouvernance unifiée de l'identité et des accès (physiques et logiques) pour renforcer l'étanchéité de l'organisation

REX AIRBUS
Continuum de la sécurité physique et numérique,
continuum de la gestion des risques et des crises

Dans le cadre industriel d'Airbus, la gouvernance de la sécurité numérique se trouve rattachée à la direction du Chief Security Officer Group (CSO), Pascal Andreï.

La mission du CSO est triplement transversale et couvre avec continuité la sûreté physique et numérique, la détection des actes malveillants et la gestion de crise, tout en supervisant par le haut les trois verticales commerciales (Commercial Aircraft, Helicopters et Defence & Space, avec intrication du civil et du militaire dans chaque division) en matière de sûreté.

La construction de la gouvernance de la sûreté chez Airbus s'est faite de manière progressive et historiquement à partir du pôle sûreté et des actifs propres au groupe :

1. Juillet 2017 : création de la Corporate Security, intégrant la sûreté physique et numérique (bases communes, gestion des risques, des vulnérabilités et des incidents). Définition d'une première feuille de route sur 5 ans, avec la Stratégie 2017-2022 visant dans un premier temps à mettre en œuvre une gouvernance par projets au sein des divisions.
2. 2019 : intégration de la gestion de crise au sein de la Corporate Security.
3. 2020 : année charnière avec la création d'un poste de CISO/CSO rattaché au CEO et la mise en place d'une instance (Corporate Security Council - CSC). Auparavant, il n'y avait pas d'autorité sur les différentes divisions.
4. 2021 : distinction entre un CSO Industriel et un CSO Produits & Services.
5. 2023 : la sécurité devient le cinquième pilier stratégique d'Airbus.

Le rattachement du CSO au CEO a permis un renforcement de l'implication de la gestion de la sécurité numérique (entre autres prérogatives) dans les instances de direction (*board of committee, board of director, board audit*). D'autres instances plus descendantes permettent par ailleurs au CSO de partager la gouvernance de la sécurité numérique avec les directeurs des trois divisions (4 CEOs *Meetings*).

Le modèle de gouvernance n'est pas intégré, mais fédéré. Une seule gouvernance est prévue pour toute la définition de la politique de sûreté, et le déploiement est réalisé par les différentes équipes responsables en fonction de la nature de l'activité de sécurité en cause (engineering, support, IT, ops …).

Les méthodes de pilotage par les risques sont co-écrites avec les métiers : avec l'IT pour l'IT, l'engineering pour l'engineering etc. et ce pour l'ensemble des départements. L'alignement se fait entre le CSO et les métiers pour définir les objectifs de sécurité à viser et les priorités à donner parmi ceux-ci.

Chaque fonction est autonome pour la feuille de route propre à son domaine d'expertise et les budgets sûreté ne sont pas centralisés au sein du CSO qui coordonne les activités au plan matriciel : chaque département détient la gestion de son budget et une partie des équipes de sécurité (numérique ou physique).

Anne Tricot, Chief of Staff at Head of CSO

Michael Barthellemy, OCSSI Airbus Commercial

Olivier Pujol, VP Governance, Risk & Compliance at Airbus

REX CRÉDIT AGRICOLE

Réévaluer sa gouvernance pour intégrer les nouveaux enjeux de sécurité numérique

En matière de sécurité numérique, la menace s'intensifie et se traduit par une croissance des alertes/incidents et par une ingéniosité plus élevée des attaques, s'appuyant sur des nouveaux outils performants fondés sur l'IA (ex. scans des vulnérabilités, *deep fakes*). Les impacts s'étendent aux différents SI externes qu'une entreprise peut consommer directement ou indirectement : les attaquants visent également les prestations critiques qui présentent généralement un niveau de sécurité hétérogène. Enfin, les nouveaux besoins *business* génèrent une extension du numérique et donc de la surface d'attaque, qu'ils convient de bien gérer de bout en bout (*Security By Design*, nouveaux contrôles / scans / tests d'intrusion, détection fuites de données…). En ce sens, les équipes en charge de la détection (SOC en particulier) sont amenées à élargir leur périmètre au niveau applicatif / services métier et au-delà de la partie infrastructure.

Dans ce contexte, le Crédit Agricole a revisité sa stratégie de sécurité numérique Groupe. Parmi les orientations retenues :

- **Une supervision accrue des dispositifs de sécurité internes et externes** (évaluation des SOC en charge de la détection, audits du risque de sécurité numérique des fournisseurs critiques…).
- **L'extension de la surveillance en mode « vigie sécurité »** : elle doit permettre à la fois aux équipes de sécurité dédiées à la détection et veille (SOC / CERT) mais aussi aux CISO des entités et leurs équipes, de bénéficier d'une chaine de détection et de traitement plus large, plus profonde, plus rapide, plus efficace, notamment au moyen de nouveaux outils plus modernes et de processus plus intégrés (délais, rôles…). Les vecteurs d'attaques et de fuites de données priorisés sont : le réseau, les sites exposés sur internet, les *devices*, les bases de données, l'Active Directory, les nouveaux usages d'IA […].
- **Une rationalisation du socle commun cyber**, en matière de solutions de sécurité utilisées (contrats Groupe/référencements, Proof of Concept), de projets communs de protection des données (dont le chiffrement, l'authentification…), de projections sur les enjeux stratégiques (cryptographie post-quantique, accélération de l'IA, autonomie stratégique…)
- Si la gouvernance de la sécurité numérique a gagné en maturité dans ses strates les plus hautes (lien entre la gouvernance de la sécurité numérique et les comités exécutifs ou conseils d'administration, détermination des priorités/budgets, partage des indicateurs de risques etc.), elle doit **davantage être complétée par une gouvernance opérationnelle plus robuste et de nouveaux outils / processus à la hauteur de l'intensité de la menace et des nouveaux besoins métier**.
- L'adoption de nouveaux outils doit être adossée à une pluridisciplinarité accrue (entre équipes Data, IA, cyber, IT, métier…) et un embarquement renforcé des collaborateurs.

Franck Poli, Group Chief Information Security Officer, Crédit Agricole

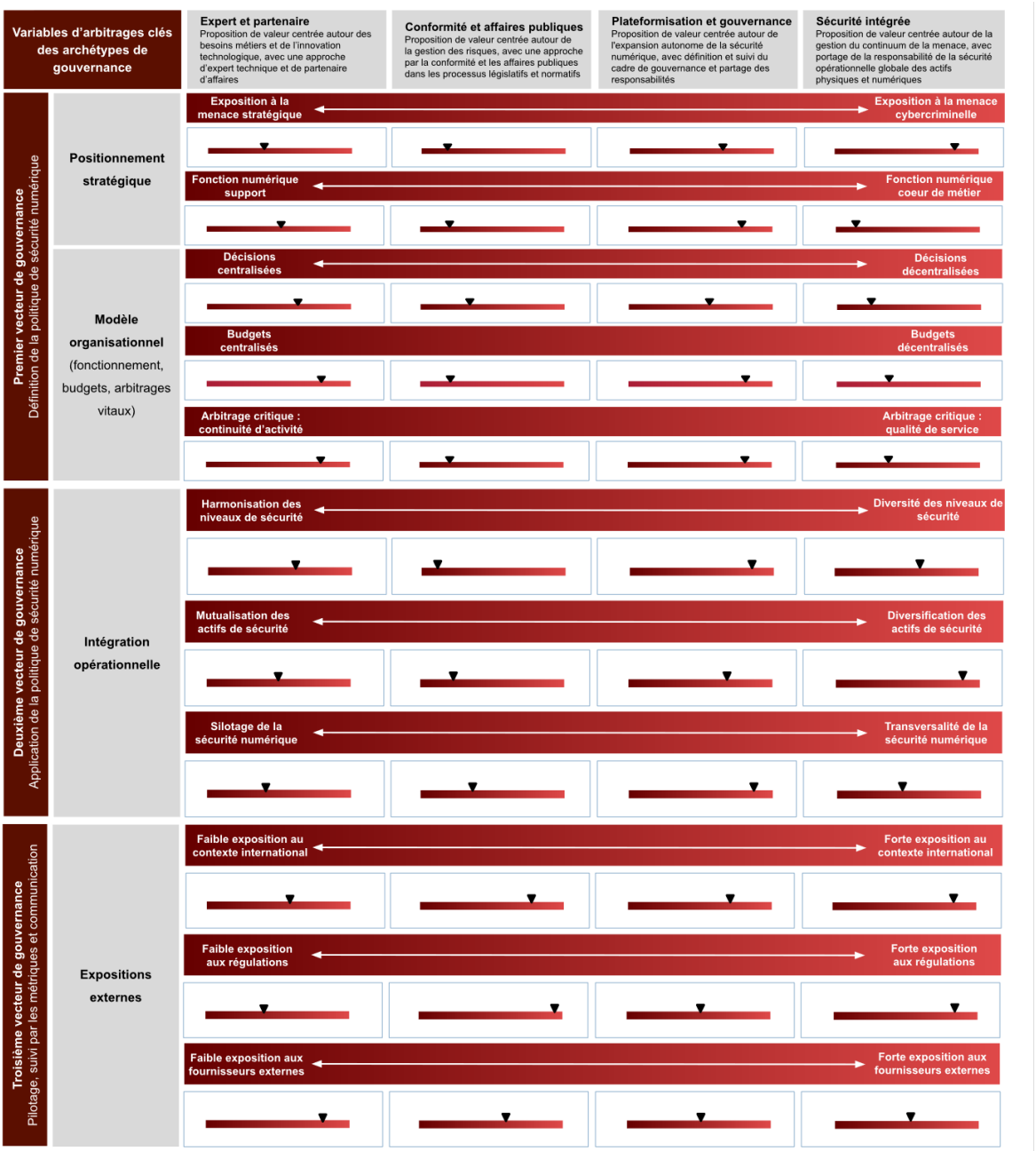


Figure 18 : Synthèse - Variables d'arbitrage clés et critères d'appréciation des 4 archétypes de gouvernance de la sécurité numérique

Equilibrer sa gouvernance	**Expert et partenaire** Proposition de valeur centrée autour des besoins métiers et de l'innovation technologique, avec une valeur ajoutée centrée sur l'expertise technique et le partenariat au service de la réussite des objectifs métiers	**Conformité et affaires publiques** Proposition de valeur centrée autour de la gestion des risques, avec une valeur ajoutée centrée sur une recherche de conformité maximale et la capacité à contribuer directement aux processus législatifs et normatifs associés, dès leur élaboration	**Plateformisation et gouvernance** Proposition de valeur centrée autour d'une offre de service interne large et performante de sécurité numérique, associée à la définition et au suivi d'un cadre de gouvernance et de partage des responsabilités avec les métiers	**Sécurité intégrée** Proposition de valeur centrée autour de la gestion intégrée du continuum de la menace, avec portage de la responsabilité de la sécurité opérationnelle globale des actifs physiques et numériques
Points de différenciation	• Crédibilité des décisions prises • Fiabilité des solutions déployées • Agilité face aux demandes d' évolutions technologiques	• Transformer la contrainte réglementaire en barrière à l'entrée • Connaissance parfaite du patrimoine informationnel et contrôle rigoureux • Anticipation et orientation des lois de sécurité numérique	• Proposition d'un catalogue de services mutualisés • Combinaison d'expertise technique et de compétences de gestion • Distribution de la sécurité dans les coeurs de métiers	• Vision à 360° de la sécurité • Culture opérationnelle du "Command & Control" • Mutualisation des outils de surveillance et des renseignements sur le continuum de la menace
Points de vigilance	• Conflit d'intérêt technico-commercial • Posture réactive de prestataire interne • Déploiement transversal des solutions	• Lourdeur procédurale sur les TTM et les innovations métiers • Illusion d'une sécurisation par les seuls efforts de mise en conformité • Inflation des budgets (audits et reporting)	• Complexité matricielle dans la décentralisation des responsabilités • Coût total de maintien d'un panel d'offres de service internes • Exposition politique de la sécurité numérique	• Dialogue et culture commune entre fonction numérique et sûreté • Sous-estimation des spécificités techniques de la sécurité numérique • Risque de "Shadow IT"
Facteurs clés de succès	• Anticiper la valeur des développements technologiques • Être force de proposition pour les architectures sécurisées • Traduire dans un langage COMEX les enjeux	• Industrialiser les processus de mise en conformité • Gestion par l'impact pénal et réputationnel • Valorisation des certifications techniques obtenues	• Définir sans ambiguïté les responsabilités des entités • Incarner la sécurité numérique au-delà de l'expertise technique • Indicateurs de performance et de risques orientés business	• Développer une culture de sécurité commune • Mettre en place une gouvernance unifiée de l'identité et des accès • Recruter des profils hybrides

Figure 19 : Synthèse - Analyse des positionnements stratégiques des 4 archétypes

3.3 RÉÉVALUATION RÉGULIÈRE DE SON MODÈLE ORGANISATIONNEL

Les évolutions technologiques conduisent à réévaluer régulièrement les modèles organisationnels.
La gouvernance de la sécurité numérique se trouvant au cœur des enjeux de gouvernance globale, de stratégie numérique et de gestion des risques, les événements charnières suivants sont propices à réorientation, au-delà de la comitologie dédiée :

- **Revues stratégiques de la politique de gouvernance**, et en particulier de la gouvernance de la sécurité ;
- **Mise à jour de la stratégie à l'échelle du groupe**, et en particulier de la stratégie numérique ;
- **Mise à jour des chantiers majeurs de transformation et de gestion des risques.**

Il semble que d'autres événements peuvent susciter la réévaluation de la gouvernance de la sécurité numérique et notamment :

- **L'évolution du poids du numérique dans les métiers et son intégration aux cœurs de métier**, la transversalité des activités numériques débordant alors le périmètre fixé hiérarchiquement par l'entité à laquelle elle était subordonnée ;
- **La mise en commun d'outils qui harmonisent les différences technologiques des entités** (CRM, ERP etc.) ;
- **Le changement à l'échelle de l'organisation de ses sous-jacents numériques**, avec un effet conséquent sur les budgets numériques (ex : modification substantielle de sa politique *corporate* de multi cloud et conséquences notables sur le P&L numérique en raison des nouveaux modèles d'affaires cloud-IA).
- **La diffusion systémique d'un ensemble d'une ou plusieurs nouvelles technologies** qui implique la transformation des processus métiers et des modes de travail, comme le laissent présager les révolutions IA.

4 PRINCIPES D'ACTIONS POUR UNE GOUVERNANCE PERFORMANTE ET COMPÉTITIVE

4.1 CONSTRUCTION DE LA PSN - FAIRE PRIMER RÉALISME ET COOPÉRATION AVANT TOUTE SOLUTION TECHNIQUE

Définir sa PSN (politique de sécurité numérique) demande d'avoir bien défini plusieurs paramètres essentiels à tout dialogue productif et de confiance avec les instances décisionnaires et opérationnelles. L'enjeu est de co-construire la PSN avec les parties prenantes sur les trois lignes de maîtrise, éventuellement à l'aide d'un RACI, pour garantir sa cohérence avec la gouvernance globale, sa communicabilité et surtout, son applicabilité réelle.

4.1.1 RÉALISME DE LA PSN : S'ALIGNER SUR LES CRITÈRES ESSENTIELS ET DIFFÉRENCIANTS DE CRÉATION DE VALEUR

4.1.1.1 Principes d'action

Pour que la sécurité numérique soit perçue par les métiers comme un véritable partenaire proactif, elle doit adopter une grammaire commune avec le reste de l'organisation. Plusieurs principes sont à « intégrer nativement », et notamment ceux qui consistent à :

- **S'approprier le modèle de création de valeur de l'organisation,** dans le but de partager de manière différenciée des objectifs et des critères de performance en phase avec ceux des conseils d'administration, des comités exécutifs et des équipes métiers ou opérationnelles.
- **Cartographier la criticité tout au long des chaînes d'activités**. Des indicateurs quantitatifs (chiffre d'affaires, marge, P&L etc.) et qualitatifs (criticité d'un produit, d'une solution ou d'un fournisseur même petit etc.) permettent de définir le risque résiduel accepté, la classification de la criticité des actifs, et l'intensité de la sécurisation attendue.
- **Démontrer la contribution concrète de la sécurité numérique à la valeur ajoutée de l'organisation** (que ce soit par sa valorisation, sa capture, son renforcement ou sa création), en dépassant les seuls aspects techniques et réglementaires.

4.1.1.2 Points de vigilance

De la même manière, il faut « prévenir nativement » plusieurs écueils et notamment :

- **Dépasser l'illusion de la conformité,** car être « en règle » ne signifie pas être pleinement protégé. La PSN ne doit pas épuiser les ressources de l'organisation en « protégeant la conformité » (en produisant de la documentation), au détriment d'actions vitales qui permettraient d'être « conformément protégé ».
- **Neutraliser les injonctions contradictoires liées à la création de valeur**, qui surviennent lorsque les schémas de rémunération, les délégations de pouvoir et les impératifs de délais (échéances, projets)

entrent en conflit avec l'ambition de sécurité affichée. Résoudre ce biais est l'un des objectifs de la mise en cohérence de la PSN avec les autres formes de gouvernance de l'organisation.

4.1.2 COOPÉRATION INTERNE : DÉCLOISONNER ET RESPONSABILISER AU BON NIVEAU LES PARTIES PRENANTES

4.1.2.1 Principes d'action

La résilience offerte par la sécurité numérique repose sur la clarification des responsabilités, la fluidité des échanges et l'entraînement conjoint entre les différentes strates de l'organisation.

En premier lieu, la résilience par la sécurité numérique exige une coordination entre le conseil d'administration, le comité exécutif et la fonction numérique, à travers les actions suivantes :

- **Mener des revues fréquentes et approfondies de la sécurité numérique**. La bonne hiérarchisation des risques exige un examen réel au plus haut niveau, et la mise en place de seuils d'alerte en phase avec l'appétence au risque du groupe.
- **Exiger la transparence absolue des indicateurs**. Les métriques « pastèques » (vertes à l'extérieur, rouges à l'intérieur) sont à bannir au profit d'indicateurs reflétant la réalité de l'exposition, seul fondement d'une véritable relation de confiance à double sens.
- **Développer un langage commun et un programme de formation et d'exercices conjoints.** L'enjeu est de traduire les défis techniques en responsabilités légales et en impacts stratégiques et business, tout en s'adaptant aux différents interlocuteurs. Cela permet également de satisfaire à l'exigence réglementaire (NIS 2) de formation des mandataires sociaux, indispensable à la validation éclairée des mesures de gestion des risques.
- **Formaliser les processus d'homologation.** Le transfert de responsabilité et la décentralisation partielle des décisions vers les métiers doivent être assumés comme des choix stratégiques, et non pas seulement comme ces adoptions techniques « par défaut ».
- **Encadrer de manière responsable l'intégration des technologies d'intelligence artificielle sur toutes ses couches (RAG, Agents, MCP, A2A).** La gouvernance de la sécurité numérique doit prendre en compte un cadre d'adoption technologique sécurisé, face à la délégation croissante de tâches critiques à des systèmes autonomes d'IA agentique qui soulève des interrogations majeures sur la responsabilité humaine. Une démarche de co-construction rigoureuse et transparente doit pouvoir favoriser les initiatives numériques métiers au service de l'innovation, de la performance et de la compétitivité, tout en contrant efficacement les pratiques illégales de « *Shadow IT* » et de « *Shadow AI* ».
- **Clarifier le partage des responsabilités relatives à la donnée avec les différentes parties prenantes : DPO** (Délégué à la Protection des Données), **Data Owners** (garant de la propriété de la donnée) et **Data Stewards** (garant de la qualité des données). La sécurité numérique ne doit pas porter seule la charge de la qualification de la donnée. Elle doit pouvoir inscrire son action dans une gestion globale des identités et des accès (IAM) pilotée de manière cohérente.

En deuxième lieu, la résilience par la sécurité numérique requiert une coordination entre la direction générale, la communication et la fonction numérique. La communication de crise [19] est un levier de résilience qui ne doit pas être improvisé, le silence étant souvent jugé plus sévèrement que la vulnérabilité elle-même. Une stratégie efficace repose sur une transparence proactive envers toutes les parties prenantes et exige de pouvoir :

- **Anticiper la paralysie et « l'effet de sidération » induit par la crise,** par la préparation de canaux alternatifs sécurisés (hors bande) et la pré-rédaction de messages types (factuels, pédagogiques, empathiques). Cette démarche est indispensable pour respecter les courts délais de notification réglementaires (alerte précoce sous 24h et notification intermédiaire sous 72h pour les entités régulées suivant l'article 23 de NIS2). De plus, cette anticipation est le moyen d'intégrer au sein des architectures numériques et des usages de services critiques des « modes dégradés d'activité », au cœur des plans de continuité d'activité (PCA) et de relance d'activité (PRA).
- **S'entraîner régulièrement pour fluidifier les réflexes** (*driller)* à travers la réalisation d'exercices de crise conjoints réunissant dirigeants, communicants et fonction numérique.
- **Intégrer nativement l'expertise cyber au sein de la cellule de communication de crise** [20]**.** Cela passe également par la désignation d'un « officier de liaison » (ou « interprète ») chargé de traduire en temps réel les impacts techniques de la cellule opérationnelle en enjeux stratégiques pour la cellule décisionnelle, évitant ainsi la paralysie par incompréhension mutuelle.

4.1.2.2 Points de vigilance

Une gouvernance de la sécurité numérique au service de la résilience doit pouvoir :

- **Clarifier la délégation et le portage des responsabilités.** Cet acte, encadré par la PSN et la mise en conformité préalable, devient décisif pour les directeurs métiers (département, filiale, région ou pays), notamment dans le cadre des homologations. Sans tiers de confiance indépendant pour objectiver le risque, un conflit d'intérêts peut s'installer, favorisant les avantages économiques de court terme au détriment de la sécurité réelle et pérenne.
- **Renforcer le maillon faible.** Il faut s'assurer que la gouvernance irrigue l'ensemble des strates de l'organisation, et non les seules instances dirigeantes. De nombreuses attaques passent simplement par un manque d'hygiène numérique des collaborateurs, indépendamment de leur niveau hiérarchique.

4.1.3 COOPÉRATION EXTERNE : CONSTRUIRE UNE DÉFENSE COLLECTIVE

4.1.3.1 Principes d'action

Les organisations actuelles ne peuvent rester des citadelles isolées. La coopération, à travers des échanges et des exercices communs, doit pouvoir s'étendre à des acteurs externes afin de :

- **Partager des capacités de défense avec les pairs du même secteur ou de la filière numérique**. Le partage de compétences et d'expertises entre acteurs permet la diffusion de bonnes pratiques inter-

[19] Voir le rapport de l'ANSSI, *Anticiper et gérer sa communication de crise cyber*, Décembre 2021
[20] Voir le rapport de l'ANSSI, *Crise cyber, les clés d'une gestion opérationnelle et stratégique*, Décembre 2021

entreprises et l'amélioration concrète de la résilience au niveau du secteur d'activité ou de l'ensemble de la filière numérique. Le partage d'informations techniques (flux CERT/CSIRT) est, en particulier, au cœur de cette dynamique collective. Dans le cadre de la cyberguerre, il représente même pour certains acteurs l'élément différenciant de leur stratégie.

Pour tirer toute la valeur de ce précieux partage d'informations, il faudrait que ces marqueurs techniques (IoC) soient traduits en impacts stratégiques et présentés dans une surcouche accessible à d'autres acteurs. L'enjeu est d'arriver à contextualiser l'information dans un espace de confiance pour que chaque acteur puisse en extraire l'impact *business*, permettant ainsi sa remontée intelligible aux décideurs. La déclinaison opérationnelle pourrait prendre pour modèle la procédure Vigipirate, avec une codification couleur des alertes selon le niveau d'urgence, et une temporalité de transfert différenciée selon interlocuteurs.

- **Responsabiliser les fournisseurs critiques**, pour refuser l'internalisation par l'organisation des risques tiers. Il s'agit alors de fluidifier sa gouvernance par des clauses en miroir (droit d'audit, délais de notification, exigences de sécurité équivalentes et natives), de clarifier les responsabilités des parties prenantes externes et de faire de la sécurité un prérequis commercial non négociable. L'intégration systématique d'un Plan d'Assurance Sécurité (PAS) permet, par exemple, de définir contractuellement la réversibilité et la garantie d'effacement des données en fin de contrat, et d'imposer un alignement strict sur les délais de notification d'incidents (comme les **4h/24h de DORA** ou les **72h du RGPD**, en complément de NIS 2).
- **Se coordonner avec les opérateurs critiques à l'échelon national**. Cette alliance prévient les attaques systémiques croisées portant atteinte aux intérêts essentiels de la nation. Cette coopération de haut niveau implique une collaboration de confiance avec les autorités de régulations (l'ANSSI, l'ACPR, CNIL etc.) et pour la dimension politique, avec les préfectures.

4.1.3.2 Points de vigilance

Pour veiller à ce que la gouvernance de la sécurité numérique intègre une dimension collective, il convient de :

- **Sécuriser juridiquement le partage d'information en temps de crise**. Cela passe notamment par l'établissement d'une charte de transmission signée par les instances dirigeantes (Comex/CA) dès le « temps froid ». Cette délégation de responsabilité pré-validée est indispensable pour autoriser les équipes opérationnelles (CSIRT) à échanger des données critiques avec l'ANSSI et les pairs de confiance sans délai. Elle lève ainsi les freins de la validation hiérarchique en pleine crise et enrichit considérablement la défense collective de l'écosystème.

REX ANSSI

Facteurs clé de succès de la gouvernance de la sécurité numériques des Jeux Olympiques de Paris 2024 : le facteur humain

La réussite de la sécurisation numérique des Jeux Olympiques et Paralympiques de Paris 2024 a démontré que la robustesse d'un dispositif ne réside pas seulement dans son volet technologique, mais également dans la coordination du collectif et le partage d'objectifs communs. La capacité de résilience s'est forgée bien en amont de l'événement, autour d'un programme en 6 axes :

Cette préparation de près de deux années avec une logique de priorisation de l'effort en fonction de la criticité des entités pour les Jeux ainsi que des entraînements communs (exercices, kits), visant à créer des automatismes de réaction face à l'imprévu, ont été des facteurs clés de réussite des JOP24 sur le volet cyber.

Le dispositif s'est appuyé sur une répartition sectorielle et géographique des CSIRTs des organisations, permettant de contextualiser la menace et de remonter les signaux faibles au plus près du terrain, à partir des connaissances des métiers.

Le partage d'information entre les acteurs français comme avec nos partenaires européens a été clé, il s'est appuyé sur des processus et canaux de communications simples, déjà utilisés par les acteurs (groupes Tchap pour partager les informations par exemple), ce qui a permis de surmonter la complexité des environnements métiers et les défis d'une harmonisation à outrance, en misant d'abord sur des manières d'être et de faire.

Cette dynamique a permis de fluidifier les chaînes de décision et de tisser, avant l'épreuve, les liens de confiance indispensables. Pendant les épreuves, la communication a permis, pour une matière encore difficile à appréhender par tous, de rassurer et d'éviter l'emballement, de sensibiliser et de se focaliser sur ce qui est le plus important.

Les Jeux Olympiques et Paralympiques 2024 ont créé un *momentum* qui a réellement permis de rehausser le niveau de sécurité de tous.

Vincent Strubel, Directeur général de l'ANSSI

4.2 MISE EN APPLICATION AU QUOTIDIEN - ALIGNER LE DISPOSITIF AVEC L'ORGANISATION EXISTANTE

Le défi principal est de trouver un équilibre dynamique entre les obligations associées au cadre de la gouvernance de la sécurité numérique et sa nécessaire flexibilité pour s'harmoniser avec les autres gouvernances de l'organisation. L'accompagnement et la mise en application concrète doivent à ce titre s'opérer par un dialogue continu entre la fonction numérique, les instances dirigeantes et les métiers, clarifiant l'offre de service de la sécurité numérique et les solutions mises à disposition.

4.2.1 ALIGNEMENT ORGANISATIONNEL : CLARIFIER LES MANDATS ET MUTUALISER LES COMPÉTENCES

4.2.1.1 Principes d'actions

La sécurité numérique ne peut se construire en parallèle de l'organisation et son application passe par un alignement optimisant ressources et mandats dans le but de :

- **Proposer un « contrat de service » interne de la fonction sécurité du numérique.** Le rôle de la filière sécurité vis-à-vis des filiales et des métiers doit être explicitement défini pour éviter, selon un triptyque clair, les conflits d'intérêts entre les fonctions de « faiseur » (opérateur), de conseil (expert) ou de gendarme (contrôleur).

- **Coordonner effectivement les gouvernances adjacentes.** La mise en œuvre doit porter une attention particulière aux points de contact avec la gouvernance des risques, de la sécurité physique (sûreté), et de la conformité, afin d'éviter les injonctions contradictoires et les zones grises de responsabilité.

- **Surmonter la complexité réglementaire.** La mutualisation des compétences peut être privilégiée en interne (au niveau groupe ou par plaque régionale) ou par secteur (comme avec le règlement européen DORA), plutôt que par chaîne de valeur isolée. Cette mutualisation permet une collaboration entre acteurs de tailles différentes, tout en créant un intérêt économique à faciliter l'intégration native des exigences légales et la propagation des standards de sécurité numérique.

4.2.1.2 Points de vigilance

L'alignement organisationnel de la gouvernance de la sécurité numérique doit prévenir certains écueils, et notamment se mettre en capacité de :

- **Proscrire la création artificielle d'un département parallèle.** En voulant trop enrichir la fonction de sécurité numérique, l'organisation risque de créer une structure redondante qui agit comme un frein. Il convient de ne pas séparer artificiellement les décideurs des orientations techniques de ceux qui en gèrent les conséquences sécuritaires.

- **Réduire le flou entre responsabilité et exécution.** Sans mécanisme clair de délégation de pouvoir, une tension structurelle subsistera toujours dans l'exécution entre le porteur du risque (et de la responsabilité légale), le commanditaire du plan de sécurité, et le détenteur du budget final.

4.2.2 PRIORISATION OPÉRATIONNELLE : HIÉRARCHISER ET TRANCHER LES ARBITRAGES VITAUX

4.2.2.1 Principes d'action

Face à l'intensité de la menace, l'approche de l'application au quotidien doit s'apparenter à une « médecine de guerre », imposant une lucidité radicale sur certaines priorités dans le but de pouvoir :

- **Être en mesure de répondre à la question de la survie de l'organisation, le cas échéant**. L'approche d'application de la sécurité numérique par les risques doit avant tout déterminer ce qui est essentiel à la pérennité de l'organisation. Selon le seuil de risque résiduel accepté, cela peut impliquer d'accepter de ne pas être prêt sur des périmètres jugés non vitaux pour concentrer l'effort sur les actifs critiques, ou de cloisonner certains actifs ou systèmes d'actifs numériques.
- **Arbitrer entre conformité formelle et sécurité réelle.** Il est impératif de prioriser les mesures ayant un impact opérationnel direct. Les arbitrages budgétaires doivent parfois favoriser intelligemment la réduction du risque encouru. Il est à noter que pour les entités importantes (EI) ou entités essentielles (EE), l'atteinte de certains objectifs de sécurité numérique est obligatoire, conformément à la directive européenne NIS2 et à sa transposition à venir en droit français. Ces objectifs concernent l'ensemble de la surface numérique, sauf justification formelle d'exclusion de périmètre.

- **Garantir la capacité de fonctionnement en mode dégradé.** L'organisation doit s'assurer de sa capacité réelle à basculer en mode manuel en cas de panne majeure. L'objectif est d'être aussi performant dans la capacité de reconstruction (*recovery*) que dans celle de protection, ce qui implique de pouvoir tester les effets en cascade. Certaines organisations profitent déjà localement (ou expérimentalement en coopération internationale) de la technologie des jumeaux numériques pour reconstituer les effets en chaîne de perturbations sur des actifs ou systèmes critiques, dans une logique de *stress test* de leur résilience opérationnelle.

4.2.2.2 Points de vigilance

Lors de sa mise en œuvre opérationnelle, la gouvernance doit s'attacher à circonscrire les dérives suivantes :

- **Garantir l'applicabilité réelle des règles fixées par la gouvernance de la sécurité numérique**. La tolérance accordée aux délits de contournement (notamment sur les *pools* de *patch* non respectés, l'utilisation de messageries non sécurisées, le partage de données confidentielles et plus généralement les *Shadow IT/Shadow AI* critiques) affaiblit structurellement la posture de sécurité numérique. La gouvernance doit présenter des principes clairs, cohérents et stables, malgré les évolutions technologiques rapides qui rendent obsolètes les prises de position conjoncturelles et non structurées. L'objectif est de conjuguer restrictions contraignantes et encadrement intelligent

et éthique qui soutenir l'innovation et garantir la fiabilité des données, la responsabilité humaine (même partiellement déléguée), ainsi que la robustesse des modèles utilisés (en particulier pour la supervision du *Retrieval-Augmented Generation*, ou RAG). De la sorte, l'engagement des collaborateurs pourrait être stimulé en faveur d'un comportement bénéfique de « *Citizen IT/Citizen AI* ».

- **Capitaliser systématiquement sur l'expérience des crises passées**. Il est crucial d'institutionnaliser le retour d'expérience (interne ou par substitution via l'analyse des concurrents) pour capitaliser sur les événements passés et éviter que le manque de documentation, la lassitude ou l'oubli ne conduisent à la réapparition de failles déjà connues.

4.2.3 GESTION DE L'ÉCOSYSTÈME ET DU FACTEUR HUMAIN : ÉTENDRE SA VIGILANCE ET MAINTENIR SON ACTION DANS LA DURÉE

4.2.3.1 Principes d'action

L'application de la PSN ne s'arrête pas aux frontières de l'organisation, ni aux seuls aspects techniques. Elle doit pouvoir englober la chaîne de valeur étendue et les hommes qui la protègent dans le but de :

- **Refuser l'internalisation du risque tiers**. Dans les relations fournisseurs, si l'évaluation des risques est une condition d'accès au marché, il ne faut pas s'en tenir à la simple étude des vulnérabilités tierces. Il est vital d'exiger des preuves de mise en œuvre effective des bonnes pratiques, et de surveiller (dans l'esprit du règlement européen DORA par exemple) le risque de concentration lié à une dépendance excessive envers un fournisseur unique ou dominant.
- **Intégrer une lecture géopolitique des menaces**. Pour nombre d'organisations exposées sur différentes plaques géographiques, l'application de la sécurité impose une lecture géopolitique (*global derisking*). Cela peut conduire à des stratégies de « découplage local », ou de décentralisation pour certaines activités critiques (zones de conflits ou à forte instabilité juridique), afin de cloisonner les risques opérationnels.
- **Préserver la soutenabilité des charges de sécurité numériques pour les ressources humaines**. Le maintien de la compétence et de l'énergie des équipes constituant le nerf de la guerre, la gouvernance de la sécurité numérique doit pouvoir anticiper la charge mentale et la frustration potentielle des RSSI et de leurs équipes. Elle doit agir comme un régulateur pour garantir la pérennité humaine du modèle, entretenir l'état d'esprit de vigilance permanente et d'intégration des nouveautés, face à l'exigence des mesures expertes qu'aucun entraînement ne saurait épuiser.

4.2.3.2 Points de vigilance

Sur ce périmètre étendu, impliquant à la fois la chaîne d'approvisionnement et le facteur humain, la gouvernance doit se doter de garde-fous pour :

- **Maîtriser les dépendances technologiques.** L'enjeu clé réside dans l'accès pérenne aux technologies et aux marchés. L'application de la gouvernance doit veiller à ne pas créer de dépendances critiques irréversibles envers des fournisseurs dont la pérennité économique ou la loyauté géopolitique peuvent s'avérer hautement volatiles.

- **Appréhender le *continuum* entre sécurité numérique et sécurité de l'information.** L'application de la sécurité gagne à traiter conjointement sécurité numérique et information, afin de faire face aux stratégies hybrides mêlant cyberattaques et déstabilisation par manipulation informationnelle. Le bon dimensionnement du SOC et du CSIRT ainsi que la qualité de leurs interactions en interne (traitement des incidents, analyse des journaux d'événements conservés) et à l'externe (partages avec les pairs sectoriels et l'écosystème de confiance à l'échelon national et européen) constituent des éléments de résilience différenciants.

REX GROUPAMA

Un schéma organisationnel construit selon l'historique, la culture et les besoins

L'organisation de Groupama s'est historiquement développée à partir de ses Caisses Régionales, qui ont progressivement mis en place des structures mutualisées. Groupama Supports et Services (G2S) constitue aujourd'hui la concrétisation opérationnelle de cette mutualisation, en portant l'informatique communautaire et en hébergeant la fonction RSSI Groupe ainsi que les équipes opérationnelles.

Cet ancrage historique a conduit chaque entité - Caisses Régionales comme filiales - à intégrer la sécurité numérique dans son fonctionnement, ce qui a nécessité la création et l'animation d'une fonction RSSI Entreprise afin d'assurer la cohérence et l'efficacité globale du dispositif.

La sécurité numérique et la gestion du risque se situent au croisement de plusieurs enjeux fondamentaux pour Groupama. Elles couvrent notamment la protection contre les attaques (bouclier cyber), la gestion des accès, la résilience, la gouvernance, la sensibilisation des collaborateurs, la conformité réglementaire ainsi que l'évaluation de la sous-traitance.

Le dispositif de gouvernance de la sécurité numérique du Groupe s'articule autour de deux modes de fonctionnement complémentaires :

- **Un mode « *Run* »**, dédié à la réduction continue du risque.
- **Un mode « Crise »**, centré sur la réponse aux incidents et la gestion opérationnelle des situations d'urgence.

Périmètre et mise en œuvre du mode « *Run* » dans la gouvernance globale

La gouvernance repose sur une PSN structurée en deux niveaux :

1. **La fonction centrale.** Portée par le RSSI Groupe, rattaché à Groupama Supports et Services (G2S), elle définit les orientations stratégiques, en assure la responsabilité, anime les instances et coordonne l'action de l'ensemble des entités via les RSSI d'entreprise (RSSIe).
2. **La déclinaison locale.** Assurée par les RSSIe des entités, elle consiste à contribuer à la définition des orientations de sécurité du Groupe, à mettre en œuvre localement les objectifs définis et à remonter aux dirigeants de leur entité les points critiques et les besoins prioritaires.

Cette organisation requiert un équilibre permanent entre **les objectifs et exigences de sécurité** définis par la fonction centrale et relayés localement et **les impératifs opérationnels** propres à chaque entité (production, qualité de service, charge).

Le pilotage par les risques constitue un pilier de cette dynamique, d'autant plus que le numérique est fortement intégré aux activités du Groupe. La gestion des risques représente un investissement nécessaire, à la fois créateur de valeur et facteur de mutualisation et d'efficience.

Patrick Prosper, DSES - RSSI Groupe chez GROUPAMA

4.3 PILOTAGE PAR LES MÉTRIQUES - PRIVILÉGIER DES INDICATEURS CONCRETS ET CIBLÉS

Le pilotage par les métriques ne doit pas être une fin en soi, mais un levier de décision stratégique. Il permet d'exercer un retour sur la structure des principes de sécurité numérique et sur leur application, en couvrant l'ensemble des capacités de résilience (anticipation, adaptation, absorption, reconstruction). L'enjeu est de passer d'un *reporting* technique à un pilotage éclairé par la valeur et les risques.

4.3.1 PILOTAGE PAR LA VALEUR : ADAPTER LA MESURE AUX BONS NIVEAUX DE DÉCISION

4.3.1.1 Principes d'action

Pour que le pilotage soit efficace, il doit reposer sur une traduction des informations techniques en données stratégiques dans le but de faciliter la prise de décision. Plusieurs actions, à peu de frais, peuvent participer à cette transformation des flux de contenus en véritables actifs :

- **Aligner les indicateurs sur les enjeux business.** Cela implique de corréler les indicateurs de sécurité aux impacts métiers (arrêt de production, perte de données clients, impact réputationnel) plutôt que de présenter des volumes d'attaques techniques bruts. Cela suppose d'intégrer les données de la CTI (*Cyber Threat Intelligence*) non comme de simples flux techniques, mais comme un outil d'aide à la décision stratégique permettant d'anticiper les menaces sectorielles spécifiques et d'ajuster dynamiquement la posture de risque.
- **Différencier les tableaux de bord selon l'audience.** Le pilotage doit fluidifier la gouvernance en faisant remonter le type et le degré d'information requis (risques majeurs, performance du programme et maîtrise du quotidien) au bon niveau de décision :
  - **Synthétiser, pour le comité stratégique**, à l'aide d'une dizaine de KPI :
    - Les tendances majeures des menaces qui exposent l'organisation (tactiques, techniques et procédures) et les actifs visés ;
    - L'état de maturité de la sécurité numérique par catégorie d'action (Identification, Protection, Détection, Réponse, Remédiation) ;
    - La fenêtre critique de vulnérabilité (ratio surface d'exposition/taux de couverture) ;
    - L'avancement pluriannuel des objectifs.
  - **Piloter, pour le comité décisionnel,** une vision « portefeuille » pour s'assurer que les budgets alloués se traduisent par une délivrance effective de nouvelles capacités de sécurité numérique. Le tableau de bord doit mesurer l'efficacité du dispositif de résilience (vitesse d'absorption et de restauration suite à un incident), et guider les arbitrages budgétaires trimestriels nécessaires à la gestion de la dette de sécurité.
  - **Monitorer, pour le comité opérationnel,** une vision « terrain » des résultats, en suivant l'avancement concret des tâches techniques, la réactivité quotidienne face aux alertes et la

capacité à « réparer les trous plus vite qu'ils n'apparaissent » pour éviter toute dégradation par obsolescence.

- **Viser une amélioration continue et mesurable**. La gouvernance de la sécurité numérique doit pouvoir répondre factuellement et positivement aux questions : « Sommes-nous suffisamment bien protégés ? » Et, « le sommes-nous aussi bien que les autres ? ». Le recours à des *benchmarks* sectoriels pertinents, assurés par des tiers de confiance (comme un assureur doté d'une entité dédiée à la sécurité numérique), constitue un outil puissant pour situer le niveau d'investissement et de maturité de l'organisation face à ses pairs.

4.3.1.2 Points de vigilance

La construction de ce pilotage par la valeur nécessite de prêter une attention particulière à l'équilibre des messages, dans le but de :

- **Maintenir l'équilibre entre la valorisation des acquis et le maintien de l'état de vigilance.** Une tension permanente existe entre le besoin de rassurer les dirigeants sur les progrès de la sécurisation et la nécessité d'alerter sur les besoins vitaux d'investissement face à la massification des menaces. Pour éviter l'écueil d'une posture alarmiste (« phénomène de Cassandre ») ou d'une fausse réassurance, le discours doit être factuel, traduit en un langage économique et orienté vers la solution (ratio coût du sinistre *versus* coût de la protection).

4.3.2 PERFORMANCE OPÉRATIONNELLE : MAÎTRISER SA DETTE TECHNIQUE ET ENTRETENIR SA RÉACTIVITÉ

4.3.2.1 Principes d'action

Le pilotage opérationnel doit viser la maîtrise concrète de la surface d'attaque, de la dette technique, des risques émergents et des signaux faibles, à travers trois impératifs :

- **Maîtriser la « dette de sécurité »**, en s'assurant que l'organisation « répare les trous » de sécurité numérique plus vite qu'ils n'apparaissent. Il convient de suivre des indicateurs de « *Lead & Lag* » (vitesse de déploiement des correctifs vs volume de nouvelles vulnérabilités) pour éviter la dégradation du niveau de sécurité par obsolescence et l'accumulation de failles. Le non-respect des standards d'hygiène doit également être suivi, en considérant par exemples les authentifications multifacteurs (MFA, pour les accès distants) ou le chiffrement (en particulier des disques des postes nomades), imposés notamment par l'article 21 de la directive européenne NIS2.
- **Mesurer l'efficacité réelle des couches de protection**. Au-delà de l'existence des outils, il faut en évaluer l'étanchéité (modèle du Reason, dit « *Swiss Cheese* »). Cela suppose de qualifier la performance avec des indicateurs en valeur absolue (ex : temps moyen de détection et de réponse) plutôt qu'avec de simples taux de conformité déclaratifs.
- **Garantir la couverture des risques inconnus**. Le pilotage doit intégrer des dispositifs couvrant les risques non scénarisés et en évaluer la performance. Cela implique de mesurer la capacité de l'organisation à basculer en mode dégradé et à reconstruire ses systèmes (capacité de *Recovery*), par des tests de restauration réguliers, allant au-delà des PCA/PRA classiques. La démarche pourrait

s'inspirer du pilotage des écarts imposé par la réglementation DORA pour les processus critiques, entre objectifs de temps de récupération (RTO) et objectifs de perte de données maximale admissible (RPO).

4.3.2.2 Points de vigilance

La mesure de la performance opérationnelle doit dépasser les biais managériaux et maintenir un état d'esprit critique pour :

- **Veiller à la représentativité réelle des indicateurs.** Les métriques qui reflètent la conformité formelle ne doivent pas supplanter celles qui rendent compte de la réalité opérationnelle, au risque de piloter une gouvernance de papier. Un tableau de bord ne doit pas masquer les zones de non-qualité ou les exceptions, sous peine de rendre l'organisation aveugle aux risques systémiques.

4.3.3 COMMUNICATION DÉCISIONNELLE : PARTAGER LES RÉSULTATS DANS UN CADRE DE CONFIANCE ET AVEC UNE VISION SYSTÉMIQUE

4.3.3.1 Principes d'action

La communication autour des métriques doit servir à fluidifier la prise de décision et à éclairer les zones d'ombre de l'organisation par les actions suivantes :

- **Identifier et traiter les maillons faibles en toute transparence.** La question suivante doit être posée et traitée en confiance : quels sont les périmètres les moins maîtrisés ? Le pilotage doit mettre en lumière de manière proactive les zones de moindre vigilance et les risques liés aux opérations de M&A en cours, aux filiales éloignées, ou aux fournisseurs critiques présentant un niveau de maturité hétérogène.

- **Prouver le rendement et la valeur ajoutée des services internes.** Dans une logique de « contrat de service », le pilotage doit permettre de démontrer la valeur ajoutée des services de sécurité (SOC, CSIRT) auprès des métiers, et notamment que les investissements réalisés permettent non seulement d'éviter des coûts (sinistres), mais aussi de garantir la continuité et la qualité de service attendue par les clients.

- **Assurer la cohérence et la fiabilité documentaire.** Fluidifier la remontée d'information exige une cohérence parfaite entre les différents documents de pilotage (cartographie des risques, PSN, tableaux de bord). Cette fluidité doit s'accompagner d'un protocole de qualification des alertes partagé avec le Comex, permettant de déclencher des réflexes décisionnels immédiats sans aucune ambiguïté sur la gravité de la situation.

4.3.3.2 Points de vigilance

La communication des métriques doit être seulement le fruit d'un long processus de structuration de la gouvernance. Il convient donc de :

- **Veiller à une qualification effective des risques avant tout pilotage par les métriques.** Vouloir mettre en place des indicateurs sans avoir réalisé au préalable une cartographie précise des activités

métiers et une qualification des risques (analyse de scénarios) est un écueil fréquent. Les métriques ne doivent pas piloter la stratégie, c'est la stratégie (basée sur les risques métiers) qui doit dicter les métriques à suivre.

REX GETLINK

Piloter sa gestion des risques par les métriques

L'activité industrielle de Getlink fait de la gestion des risques une approche naturelle à tout pilotage d'activité et fonde un modèle organisationnel dans lequel le *Chief Digital Officer* assume la double responsabilité de Directeur de la fonction numérique et de Directeur de la sécurité numérique.

Pour répondre aux attentes des comités exécutifs et des conseils d'administration, il faut pouvoir être en mesure d'apporter des éléments raisonnables à la question « De quoi dois-je avoir peur ? ». Deux questions relatives à la mesure du niveau de protection en découlent :

- « Sommes-nous suffisamment bien protégés ? »
- « Et le sommes-nous aussi bien que les autres acteurs ? »

Ce questionnement initial a la vertu d'objectiver la qualité de l'application de la politique de sécurité numérique au quotidien et de partager régulièrement un état des lieux avec les directions métiers, en les responsabilisant sur leurs périmètres d'action. Il est le fondement du pilotage de la sécurité numérique par les métriques, qui vient objectiver un ensemble cohérent de politiques, de principes d'architecture, de procédures, de gestes du quotidien et d'outils propre à chaque organisation. À ce titre, chaque couche entre la menace, l'incident et les conséquences sont dépendantes du contexte d'opération. La comparaison inter-sectorielle peut donc s'avérer trompeuse et doit bien être resituée dans son contexte, en fonction des besoins et des activités réelles de chaque acteur.

Chaque couche de protection possède des failles inhérentes, certaines connues et assumées dès la conception, d'autres moins bien maîtrisées et qui peuvent évoluer dans le temps. Le bon pilotage par les métriques repose donc au préalable sur le fait de recenser, en impliquant les métiers, les couches mises en place dans son organisation et de qualifier le niveau d'étanchéité de ces couches, selon le modèle de Reason, dit *Swiss Cheese Model* (SCM). Chez Getlink, la partie KPI vise principalement les couches basses de la sécurité numérique : principes de base et hygiène numérique, d'une part, cadre réglementaire et normatif, d'autre part. Un dispositif complémentaire à cette approche par la conformité consiste à apprécier les risques numériques par la création de scénarios plus complets.

À cela s'ajoute un indicateur propre à Getlink qui cherche à mesurer la surface des « trous » des couches de sécurité numérique. Les principes sont les suivants :

- Plus c'est bas, mieux c'est.
- La mesure doit être en valeur absolue.
- La surface est proportionnelle au risque induit.
- Les trous alignés doivent être autant que possible surpondérés.

- Les mesures (et non les estimations !) doivent être redondantes pour le « *Lead & Lag* », en mesurant par exemple le *patching* et les vulnérabilités. L'objectif est de couvrir le périmètre total, par une multiplicité de lectures qui permette d'adresser l'ensemble.

5 Indices de sécurité numérique sont déjà mis en place et concernent aussi bien les *endpoints* (en live) que les serveurs et services cloud (en live), le réseau (en mode projet), le *phishing* (en live) et l'applicatif (en mode projet).

Les coûts induits par la mise en place d'outils de mesure sont marginaux par rapport à ceux qu'impliquent les programmes de remédiation. Ils couvrent l'ensemble des lignes de défense et leur partage répond aux différents niveaux de la comitologie.

Frédéric Riga, Chief Digital Officer chez GETLINK

CONCLUSION

Nous espérons avoir pu souligner par ce rapport que la gouvernance de la sécurité numérique est un enjeu majeur qui ne peut pas se traiter à la légère, ou selon un modèle unique, tant il relève de choix stratégiques à assumer.

Nous espérons avoir donné des pistes pour structurer l'action des décideurs, notamment autour des trois vecteurs de gouvernance, pour la construction éclairée d'une politique de sécurité numérique (PSN), pour son application rigoureuse au quotidien et pour son pilotage par des métriques d'aide à la décision.

Nous espérons avoir pu tirer parti des contraintes du contexte extérieur pour faire de la résilience globale un atout de confiance et de compétitivité pour les organisations françaises, publiques comme privées.

Il appartient désormais aux dirigeants d'incarner et de porter cette culture de la vigilance à tous les échelons, pour faire de la sécurité numérique le socle robuste et vertueux sur lequel pourraient se bâtir, en toute sérénité, les innovations de demain, au service du bien commun.

Cigref
RÉUSSIR
LE NUMÉRIQUE

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

Appartenance
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence
Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr

Cigref
RÉUSSIR
LE NUMÉRIQUE