AYI NEDJIMI Consultants

Gouvernance cybersécurité : rôle du RSSI et du COMEX

Catégorie : Consulting Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Structurez la gouvernance cybersécurité au niveau du COMEX. Rôle du RSSI, comités de pilotage, reporting direction et obligations NIS 2 décryptées.

Résumé exécutif

La gouvernance de la cybersécurité au plus haut niveau de l'organisation est devenue une exigence incontournable portée par la directive NIS 2 qui impose explicitement la responsabilité du management dans la supervision des mesures de gestion des risques cyber. Ce guide analyse en profondeur le rôle stratégique du RSSI comme interface entre la technique et le business, les mécanismes de gouvernance formalisés à mettre en place pour impliquer activement le COMEX dans les décisions structurantes de cybersécurité, les modèles de reporting adaptés aux attentes spécifiques des dirigeants non techniques et les bonnes pratiques organisationnelles éprouvées permettant de transformer la cybersécurité d'un centre de coûts techniques perçu comme une contrainte opérationnelle en un véritable levier de création de valeur, de confiance numérique et de différenciation compétitive pour l'ensemble de l'écosystème de l'organisation dans un marché où la confiance numérique devient un avantage concurrentiel déterminant.

La cybersécurité ne peut plus rester cantonnée dans les sous-sols de la direction des systèmes d'information, portée par un RSSI isolé qui peine à se faire entendre au-delà du périmètre technique de la DSI. Les régulateurs européens l'ont compris et codifié dans la directive NIS 2 qui impose désormais aux organes de direction des entités essentielles et importantes d'approuver les mesures de gestion des risques cyber, de superviser leur mise en œuvre effective et de suivre des formations régulières en cybersécurité sous peine de sanctions personnelles. Le règlement **DORA** va encore plus loin pour le secteur financier en exigeant que l'organe de direction définisse, approuve et supervise activement la stratégie de résilience opérationnelle numérique. Cette évolution réglementaire majeure traduit une réalité que les organisations les plus matures avaient déjà intégrée depuis longtemps : la cybersécurité est un enjeu stratégique de gouvernance d'entreprise, au même titre que la gestion financière, la conformité juridique ou la responsabilité sociétale, et non une simple problématique technique déléguée à des spécialistes informatiques. Dans ce contexte de responsabilisation accrue du top management, le positionnement du *RSSI*, ses prérogatives, son rattachement hiérarchique et sa capacité à dialoguer efficacement avec le COMEX deviennent des facteurs déterminants de la maturité cybersécurité de l'organisation tout entière et de sa capacité à faire face aux crises numériques.

Pourquoi le COMEX doit-il s'impliquer dans la cybersécurité ?

L'implication du comité exécutif dans la gouvernance de la cybersécurité n'est plus une recommandation de bonne pratique mais une obligation légale portée par NIS 2 et DORA. L'article 20 de la directive NIS 2 stipule explicitement que les organes de direction des entités essentielles et importantes doivent approuver les mesures de gestion des risques cyber et superviser leur mise en œuvre. Les membres de la direction peuvent être tenus personnellement responsables en cas de manquement à ces obligations, avec des sanctions pouvant inclure l'interdiction temporaire d'exercer des fonctions de direction.

Au-delà de l'obligation réglementaire, l'implication du COMEX est indispensable pour plusieurs raisons stratégiques fondamentales. Les décisions de cybersécurité impliquent des arbitrages budgétaires significatifs que seule la direction peut trancher. Les choix de **tolérance au risque** cyber reflètent l'appétence au risque globale de l'organisation et doivent être cohérents avec la stratégie d'entreprise. La gestion de crise cyber nécessite une chaîne de décision rapide incluant la direction pour les communications externes, les décisions de paiement de rançon et la coordination avec les autorités. L'ensemble s'inscrit dans une démarche de conformité NIS 2 qui touche toute l'organisation.

Votre RSSI a-t-il un accès direct au COMEX ou doit-il passer par trois niveaux hiérarchiques avant que ses alertes critiques remontent à la direction ?

Comment positionner le RSSI dans l'organisation ?

Le positionnement hiérarchique du RSSI conditionne directement son efficacité et sa capacité d'influence dans l'organisation. Trois modèles principaux coexistent dans les organisations françaises. Le premier, le plus traditionnel, rattache le RSSI à la DSI : il offre une proximité technique mais crée un conflit d'intérêts structurel car le RSSI dépend hiérarchiquement de celui dont il doit auditer et challenger les choix techniques. Le deuxième modèle rattache le RSSI à la direction des risques ou à la direction de la conformité : il garantit l'indépendance mais peut éloigner le RSSI des réalités opérationnelles techniques.

Le troisième modèle, recommandé par les référentiels internationaux et de plus en plus adopté par les organisations matures, rattache le **RSSI directement au directeur général** ou au secrétaire général avec un accès régulier et non filtré au COMEX. Ce positionnement garantit l'indépendance vis-à-vis de la DSI, la visibilité au plus haut niveau et la capacité d'arbitrage rapide. Il implique cependant que le RSSI développe des compétences de communication managériale et de gestion stratégique en complément de son expertise technique. Le profil du RSSI moderne est celui d'un *risk manager* bilingue capable de parler technique avec les équipes opérationnelles et stratégie avec la direction.

Mon avis : Le rattachement du RSSI à la DSI est un modèle en voie d'extinction qui ne résiste pas à l'analyse. Comment le RSSI peut-il exercer un contrôle indépendant sur la sécurité des projets de la DSI s'il dépend hiérarchiquement du DSI ? Je recommande systématiquement un rattachement au directeur général ou au directeur des risques, avec un mandat clair validé par le conseil d'administration et une ligne de reporting directe au COMEX minimum trimestrielle.

Quels mécanismes de gouvernance mettre en place ?

La gouvernance effective de la cybersécurité repose sur un ensemble de comités et de processus formalisés qui structurent la prise de décision à tous les niveaux de l'organisation. Au niveau stratégique, le **comité cybersécurité du COMEX** se réunit trimestriellement pour valider la stratégie de sécurité, arbitrer les investissements majeurs, examiner les indicateurs de risque et prendre connaissance des incidents significatifs. Ce comité doit inclure au minimum le DG, le RSSI, le DSI, le directeur financier et le directeur juridique.

Au niveau tactique, le **comité de pilotage sécurité** se réunit mensuellement pour suivre l'avancement des projets de sécurité, examiner les résultats des audits et des tests d'intrusion, valider les dérogations à la politique de sécurité et coordonner les actions correctives. Au niveau opérationnel, les réunions hebdomadaires de l'équipe sécurité couvrent la gestion des incidents en cours, le suivi des vulnérabilités et la coordination avec les équipes du SOC. L'ensemble forme une cascade de gouvernance cohérente documentée dans une charte de gouvernance cyber validée par la direction.

Instance de gouvernance	Fréquence	Participants clés	Décisions types
Comité cybersécurité COMEX	Trimestriel	DG, RSSI, DSI, DAF, DJ	Stratégie, budget, tolérance au risque
Comité de pilotage sécurité	Mensuel	RSSI, DSI, resp. métier	Projets, audits, dérogations
Comité opérationnel sécurité	Hebdomadaire	RSSI, équipe sécu, SOC	Incidents, vulnérabilités, patches
Revue de direction SMSI	Semestriel	DG, RSSI, auditeur	Performance SMSI, amélioration continue
Cellule de crise cyber	Sur activation	DG, RSSI, DSI, DJ, COM	Gestion de crise, communication

L'attaque par ransomware contre le groupe Kaseya en juillet 2021, qui a impacté plus de 1500 entreprises à travers le monde via la compromission de la plateforme VSA utilisée par les MSP, a démontré l'importance cruciale d'une gouvernance cybersécurité impliquant le COMEX dans la gestion de crise. Les organisations dont la direction était formée et préparée aux scénarios de crise cyber ont pris des décisions rapides et coordonnées concernant l'isolement des systèmes, la communication clients et la mobilisation des ressources de réponse, tandis que celles où la cybersécurité restait cloisonnée dans la DSI ont perdu des heures précieuses en escalades hiérarchiques improvisées.

Comment structurer le reporting cybersécurité au COMEX ?

Le reporting cybersécurité destiné au COMEX doit être radicalement différent des tableaux de bord techniques utilisés par l'équipe sécurité. Les dirigeants attendent des indicateurs orientés risques métier et non des métriques techniques abstraites. Le rapport trimestriel du RSSI au

COMEX doit couvrir quatre dimensions : le **niveau d'exposition aux risques** avec une cartographie visuelle des risques majeurs et leur évolution, la **performance du dispositif de sécurité** avec des KPIs comparés aux objectifs et aux benchmarks sectoriels, l'**état de conformité réglementaire** avec les écarts identifiés et les plans de remédiation, et les **incidents significatifs** avec les leçons tirées et les actions correctives mises en œuvre.

Le format doit être synthétique et visuel, idéalement limité à cinq ou six slides maximum pour le corps de la présentation avec des annexes disponibles pour les questions de détail. L'utilisation d'un code couleur simple (rouge, orange, vert) facilite la lecture rapide et la prise de décision. Chaque indicateur doit être accompagné d'une recommandation d'action claire avec un budget estimé et un calendrier, en cohérence avec le suivi de conformité RGPD et les exigences de réponse aux incidents.

Faut-il former les dirigeants à la cybersécurité ?

La formation des dirigeants à la cybersécurité est désormais une obligation légale explicite de la directive NIS 2. L'article 20 impose que les membres des organes de direction des entités essentielles et importantes suivent des formations permettant d'acquérir des connaissances et compétences suffisantes pour identifier les risques cyber et évaluer les pratiques de gestion des risques. Cette obligation n'exige pas que les dirigeants deviennent des experts techniques, mais qu'ils comprennent suffisamment les enjeux pour exercer leur rôle de supervision éclairée.

Le programme de formation des dirigeants doit couvrir les **fondamentaux de la menace cyber** avec des exemples concrets de leur secteur d'activité, les **obligations réglementaires** et les responsabilités personnelles des dirigeants, les **mécanismes de gouvernance** et les indicateurs à surveiller, et les **bonnes pratiques de gestion de crise** cyber incluant des exercices de simulation. La formation doit être renouvelée annuellement et complétée par des exercices de crise sur table impliquant l'ensemble du COMEX, en lien avec la méthodologie de gestion de crise de l'ANSSI.

Comment mesurer la maturité de la gouvernance cybersécurité ?

L'évaluation de la maturité de la gouvernance cybersécurité s'appuie sur des modèles de maturité reconnus qui permettent de positionner l'organisation sur une échelle de progression et d'identifier les axes prioritaires d'amélioration. Le **NIST CSF** propose un modèle en quatre tiers (partiel, informé, reproductible, adaptatif) qui couvre à la fois les aspects techniques et organisationnels. Le *CMMI Cybermaturity* offre une évaluation plus granulaire en cinq niveaux avec des critères spécifiques pour chaque domaine de la gouvernance.

Les dimensions clés à évaluer incluent le positionnement et l'autorité du RSSI dans l'organigramme, l'existence et l'efficacité des comités de gouvernance dédiés, la qualité et la fréquence du reporting au COMEX, l'intégration de la cybersécurité dans les processus de gestion des risques d'entreprise, la formation effective des dirigeants et la capacité démontrée de gestion de crise cyber. L'évaluation doit être conduite annuellement et les résultats comparés

aux benchmarks sectoriels disponibles auprès d'organismes comme l'ENISA et d'associations professionnelles comme le CESIN en France. Les résultats alimentent le pilotage opérationnel de la sécurité.

Sources et références : ANSSI · CERT-FR

Comment gérer la communication de crise cyber au niveau COMEX ?

La communication de crise cyber est une responsabilité directe du COMEX qui ne peut pas être déléguée aux équipes techniques. Lorsqu'un incident majeur survient, les dirigeants doivent être en mesure de communiquer rapidement et de manière coordonnée avec les différentes parties prenantes : clients, partenaires commerciaux, autorités de régulation, médias et collaborateurs internes. Le plan de communication de crise doit être préparé en amont avec des templates de messages adaptés à chaque audience et à chaque type d'incident, validés par la direction juridique et la direction de la communication.

Les obligations réglementaires de notification imposées par NIS 2 et le RGPD renforcent l'urgence de cette préparation. L'alerte précoce aux autorités compétentes doit être transmise dans les 24 heures suivant la détection d'un incident significatif au sens de NIS 2, et la notification complète dans les 72 heures. Le COMEX doit être formé à ces obligations et disposer de fiches réflexes claires identifiant qui communique quoi, à qui et dans quel délai. Des exercices de communication de crise intégrés aux exercices de gestion de crise cyber permettent de roder les processus et d'identifier les points de friction avant qu'une situation réelle ne les révèle sous pression.

À retenir : La gouvernance de la cybersécurité au niveau du COMEX n'est plus optionnelle depuis NIS 2. Le RSSI doit être positionné avec un accès direct à la direction, les comités de gouvernance doivent être formalisés et actifs, le reporting doit parler le langage des risques métier et non de la technique, et les dirigeants doivent être formés et exercés régulièrement aux scénarios de crise cyber. La maturité de la gouvernance se mesure et se compare aux standards de l'industrie.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr