AYI NEDJIMI Consultants

Budget cybersécurité : justifier vos investissements

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

Justifiez votre budget cybersécurité auprès du COMEX. Quantification des risques, benchmarks sectoriels, ROI sécurité et argumentaire réglementaire.

Résumé exécutif

Justifier le budget cybersécurité auprès du COMEX et obtenir les investissements nécessaires est un exercice délicat qui requiert de traduire les risques techniques en enjeux financiers compréhensibles par des décideurs non spécialistes. Ce guide propose une méthodologie structurée pour construire, présenter et défendre votre budget cybersécurité en s'appuyant sur l'analyse quantitative des risques, le benchmarking sectoriel, le calcul du retour sur investissement sécurité et les obligations réglementaires qui constituent autant de leviers argumentaires pour convaincre la direction financière et le comité exécutif d'allouer les ressources budgétaires et humaines indispensables au maintien d'une posture de sécurité adaptée au niveau de menace actuel et aux exigences de conformité réglementaires applicables à l'organisation dans le contexte français et européen actuel marqué par l'entrée en vigueur de NIS 2 et de DORA.

Le budget cybersécurité demeure l'un des sujets de tension les plus récurrents entre le RSSI et la direction financière des organisations françaises et européennes en 2026. D'un côté, le RSSI fait face à une **explosion de la surface d'attaque** liée à la transformation numérique accélérée, à l'adoption massive du cloud computing, à la généralisation du travail hybride et à la multiplication des objets connectés, le tout dans un contexte de sophistication croissante des menaces où les groupes de ransomware industrialisent leurs opérations et où les attaques étatiques ciblent de plus en plus les infrastructures civiles et les entreprises stratégiques. De l'autre côté, la direction financière subit une pression constante pour optimiser les coûts, démontrer le retour sur investissement de chaque euro dépensé et prioriser les investissements en faveur de la croissance et de la compétitivité commerciale de l'organisation. Cette tension structurelle ne peut être résolue que par une *approche méthodique de justification budgétaire* qui traduit les risques cyber en termes financiers compréhensibles, s'appuie sur des données objectives et des benchmarks sectoriels crédibles, et démontre concrètement la valeur créée par les investissements de sécurité au-delà de la simple réduction du risque technique, en intégrant les obligations réglementaires croissantes comme levier argumentaire supplémentaire.

Comment quantifier les risques cyber en termes financiers ?

La quantification financière des risques cyber est la première étape pour construire un argumentaire budgétaire crédible auprès de la direction. La méthodologie **FAIR** (Factor Analysis of Information Risk) offre un cadre structuré pour estimer la perte financière probable associée

à chaque scénario de risque en combinant la fréquence estimée de l'événement et l'amplitude de la perte potentielle. Pour chaque scénario, on calcule une *Annual Loss Expectancy* (ALE) qui représente la perte financière moyenne annuelle attendue.

Les composantes de la perte à quantifier incluent les coûts directs de réponse à l'incident (forensic, remédiation, communication de crise), les coûts de perte d'exploitation (interruption d'activité, perte de chiffre d'affaires), les coûts juridiques et réglementaires (amendes RGPD, contentieux, accompagnement juridique), les coûts de réputation (attrition clients, impact sur le cours de bourse pour les sociétés cotées) et les coûts de renforcement post-incident (mesures correctives imposées par les assureurs ou les régulateurs). Cette quantification permet de comparer directement le coût d'un investissement de sécurité à la réduction de perte attendue, créant un ratio **ROI sécurité** compréhensible par la direction financière, en lien avec la cyber-assurance.

Avez-vous déjà calculé le coût financier réel d'une semaine d'interruption de votre activité principale, en incluant la perte de chiffre d'affaires, les pénalités contractuelles et l'attrition client ?

Quels benchmarks utiliser pour calibrer le budget ?

Les benchmarks sectoriels constituent un outil précieux pour positionner le budget cybersécurité de l'organisation par rapport à ses pairs et identifier les écarts significatifs. Le ratio le plus couramment utilisé est le **pourcentage du budget IT consacré à la cybersécurité**, qui se situe typiquement entre 5 et 15 pour cent selon le secteur et la taille de l'organisation. Les secteurs les plus réglementés (finance, santé, défense) se situent dans la fourchette haute, tandis que les secteurs moins exposés peuvent se positionner plus bas.

D'autres métriques de benchmarking utiles incluent le **coût de sécurité par employé** (typiquement 1500 à 5000 euros par an), le **ratio ETP sécurité / ETP total** (objectif de 1 pour 200 à 1 pour 500 selon le secteur) et le **budget sécurité rapporté au chiffre d'affaires** (0,5 à 2 pour cent pour les organisations matures). Les sources de benchmarks fiables incluent les études annuelles du CESIN, les rapports Gartner et Forrester, les enquêtes de l'ENISA et les données sectorielles des associations professionnelles. Ces benchmarks doivent être utilisés comme points de référence contextués, et non comme des objectifs absolus à atteindre mécaniquement, en articulant avec la conformité NIS 2.

Mon avis : Les benchmarks sont utiles mais dangereux s'ils sont utilisés comme unique argumentaire. Dire au COMEX que vous dépensez moins que la moyenne du secteur ne suffit pas à justifier un budget. Il faut coupler le benchmarking avec une analyse de risques quantifiée qui montre le lien direct entre le niveau d'investissement et le niveau de risque résiduel accepté. C'est cette combinaison données externes et analyse interne qui convainc les directeurs financiers les plus exigeants.

Comment structurer la présentation budgétaire au COMEX ?

La présentation budgétaire au COMEX doit être structurée comme un business case stratégique, pas comme une liste de produits techniques à acheter. La structure recommandée comprend cinq sections : le **contexte des menaces** illustré par des incidents récents dans le secteur d'activité, le **niveau de risque actuel** quantifié en termes financiers avec les scénarios critiques identifiés, les **investissements proposés** avec leur impact attendu sur la réduction du risque, le **positionnement par rapport aux benchmarks** sectoriels et aux exigences réglementaires, et le **scénario de non-investissement** décrivant les conséquences concrètes du statu quo.

Chaque investissement proposé doit être accompagné d'un **business case individuel** précisant le problème adressé, la solution retenue, le coût total (acquisition, intégration, exploitation), le bénéfice attendu en termes de réduction de risque ou de conformité, et le délai de mise en œuvre. La présentation doit proposer plusieurs scénarios budgétaires (minimal, recommandé, optimal) avec les niveaux de risque résiduel associés à chaque scénario, permettant au COMEX de faire un choix éclairé en connaissance de cause. Les informations alimentent le tableau de bord de pilotage de la conformité RGPD.

Poste budgétaire	Part typique du budget	Justification principale	ROI mesurable
Ressources humaines sécurité	35-45%	Pilotage, expertise, opérations SOC	Capacité de réponse et détection
Solutions techniques (outils)	25-35%	Protection, détection, réponse	Réduction surface d'attaque
Services externes (audits, conseil)	10-15%	Expertise spécialisée, conformité	Conformité réglementaire
Formation et sensibilisation	5-10%	Culture sécurité, réduction risque humain	Réduction incidents phishing
Assurance cyber	5-10%	Transfert de risque résiduel	Couverture financière sinistres

L'attaque par ransomware NotPetya en 2017 contre le groupe Maersk, qui a paralysé l'intégralité des opérations du géant du transport maritime pendant plus de dix jours, a généré des pertes estimées à 300 millions de dollars. Le PDG de Maersk a publiquement reconnu que l'entreprise avait sous-investi dans la cybersécurité avant l'attaque. Après l'incident, le budget cybersécurité du groupe a été multiplié par un facteur significatif, démontrant qu'il est toujours moins coûteux d'investir préventivement que de reconstruire après une catastrophe. Ce cas illustre parfaitement le coût de la non-sécurité comme argument budgétaire ultime auprès du COMEX et des équipes de réponse aux incidents.

Pourquoi les obligations réglementaires renforcent l'argumentaire ?

Les obligations réglementaires constituent un levier argumentaire puissant et souvent décisif pour obtenir les budgets de cybersécurité nécessaires. La directive NIS 2 impose des mesures de sécurité minimales dont le non-respect expose l'organisation à des sanctions financières pouvant atteindre **10 millions d'euros ou 2 pour cent du chiffre d'affaires mondial** pour les entités essentielles. Le RGPD prévoit des sanctions allant jusqu'à 20 millions d'euros ou 4 pour cent du chiffre d'affaires mondial. Le règlement DORA impose des exigences spécifiques de résilience opérationnelle numérique au secteur financier avec un régime de sanctions dissuasif.

L'argumentaire réglementaire permet de transformer certains investissements de sécurité en **obligations de conformité** non négociables plutôt qu'en choix discrétionnaires soumis aux arbitrages budgétaires habituels. Le RSSI peut ainsi présenter une partie du budget comme le coût de la conformité réglementaire, comparé au montant des sanctions potentielles en cas de non-conformité, créant un ratio coût-bénéfice extrêmement favorable. Les recommandations de l'ANSSI en matière de cyberhygiène et les standards de l'ENISA fournissent des références crédibles pour calibrer les investissements minimum requis.

Comment démontrer le ROI des investissements sécurité ?

La démonstration du retour sur investissement des dépenses de cybersécurité est l'exercice le plus délicat de la justification budgétaire, car la sécurité est par nature un investissement de prévention dont le succès se mesure par l'absence d'événements négatifs. Plusieurs approches complémentaires permettent néanmoins de quantifier la valeur créée. Le **ROSI** (Return on Security Investment) compare le coût de l'investissement à la réduction de la perte annuelle attendue (ALE avant investissement moins ALE après investissement).

D'autres indicateurs de valeur incluent la **réduction du temps moyen de détection et de réponse** aux incidents (MTTD et MTTR), la **diminution du nombre d'incidents** par catégorie, le **maintien de la conformité réglementaire** évitant les sanctions financières, le **renforcement de la confiance client** mesurable par la rétention et l'acquisition de contrats exigeant des garanties de sécurité, et l'**amélioration de la notation de sécurité** externe qui conditionne les primes d'assurance cyber et les conditions de souscription. Chaque investissement budgétaire doit être traçable vers un ou plusieurs de ces indicateurs de valeur, en cohérence avec le pilotage du SOC.

Faut-il externaliser pour optimiser le budget cybersécurité ?

L'externalisation partielle des fonctions de cybersécurité constitue un levier d'optimisation budgétaire pertinent, particulièrement pour les organisations de taille intermédiaire qui ne peuvent pas justifier le recrutement d'une équipe interne complète couvrant toutes les compétences nécessaires. Les services managés de sécurité (SOC externalisé, MDR, MSSP) permettent d'accéder à un niveau d'expertise et de couverture 24 heures sur 24 qui serait prohibitif en internalisation complète pour la plupart des ETI et grandes PME.

L'analyse make-or-buy doit cependant intégrer les coûts cachés de l'externalisation : gestion de la relation fournisseur, perte de compétences internes, risques de dépendance, délais de réponse potentiellement plus longs et contraintes de confidentialité. L'approche hybride optimale combine généralement une compétence interne forte sur la gouvernance, la gestion des risques, la conformité et le pilotage stratégique, avec une externalisation ciblée des fonctions opérationnelles à forte intensité de ressources comme la surveillance 24/7, les tests d'intrusion périodiques et la veille vulnérabilités. Cette optimisation budgétaire s'inscrit dans la démarche globale de résilience cloud.

Sources et références : ANSSI · CERT-FR

Comment planifier le budget cybersécurité sur plusieurs années ?

La planification budgétaire pluriannuelle est essentielle pour inscrire les investissements de cybersécurité dans une trajectoire cohérente et prévisible, facilitant à la fois la gestion financière et la montée en maturité progressive de l'organisation. Le plan pluriannuel, typiquement sur trois à cinq ans, doit distinguer les investissements de mise en conformité réglementaire à caractère obligatoire et non reportable, les projets de transformation structurants visant à réduire significativement le niveau de risque, les dépenses récurrentes de fonctionnement incluant les ressources humaines, les licences et les services managés, et les provisions pour incidents et adaptations nécessaires face à l'évolution imprévisible de la menace.

La trajectoire budgétaire doit être alignée sur la feuille de route de maturité cybersécurité définie avec la direction, avec des paliers de progression clairs et des livrables mesurables à chaque étape. L'approche par vagues successives permet de répartir l'effort financier tout en démontrant des résultats tangibles chaque année, maintenant ainsi le soutien du COMEX et de la direction financière dans la durée. La révision annuelle du plan pluriannuel intègre les évolutions du contexte de menace, les nouvelles exigences réglementaires identifiées et les retours d'expérience des investissements réalisés lors des exercices précédents.

À retenir : La justification du budget cybersécurité auprès du COMEX repose sur trois piliers argumentaires complémentaires : la quantification financière des risques démontrant le coût potentiel de la non-sécurité, le benchmarking sectoriel positionnant l'organisation par rapport à ses pairs et les obligations réglementaires transformant certains investissements en coûts de conformité non négociables. Structurez votre présentation comme un business case avec plusieurs scénarios budgétaires et les niveaux de risque associés pour permettre au COMEX de décider en connaissance de cause.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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