OG IT CONSULTING

LIVRE BLANC · 2026

— PROGRAMME CYBERCONFIANCE & CYBERASSURANCE

En 2026, votre cyber-risque vous rattrape de quatre façons.

Le guide stratégique des dirigeants de PME tech, SaaS et ESN pour évaluer leur exposition, devenir réellement assurables, et reprendre la main face aux clients enterprise.

ÉDITION TECH · SAAS · ESN

AUTEURE

Radia OURO-GBELE

Founder & Managing Director · OG IT Consulting · Édition Juin 2026

ÉDITO

Le cyber-risque n'est plus un sujet technique. C'est une décision de dirigeant.

En 2026, ce ne sont plus seulement les attaquants qui frappent vos systèmes. Ce sont aussi vos assureurs qui durcissent leurs questionnaires, vos donneurs d'ordre qui exigent des preuves avant de signer, et la directive NIS2 qui transfère la responsabilité jusqu'à votre comité de direction. Quatre forces, une même conséquence : le risque vous rattrape par là où vous ne l'attendiez pas.

Pendant des années, la cyber-assurance a fonctionné comme un produit financier presque banal : on souscrivait, on payait, et on espérait n'avoir jamais à activer la garantie. Cette époque est terminée. Aujourd'hui, un dossier de souscription PME sur deux est refusé ou conditionné, les franchises explosent, et un pourcentage croissant de sinistres déclarés se voit notifier des exclusions auxquelles le dirigeant ne s'attendait pas.

Ce livre blanc s'adresse aux dirigeants d'éditeurs SaaS, d'ESN et de PME tech françaises dont la crédibilité commerciale dépend désormais directement de leur niveau de cyber-maturité documentée. Il n'a pas vocation à vous faire peur. Il a vocation à vous rendre maître de votre exposition — et donc maître de votre assurabilité.

CE QUE VOUS ALLEZ EN RETIRER

Une vision claire du gap entre votre risque réel et votre couverture, les 5 questions qui changent toute négociation avec un assureur, et la méthode qui vous rend, en 10 jours ouvrés, capable de répondre à toutes vos parties prenantes.

Radia OURO-GBELE
Founder & Managing Director — OG IT Consulting

SOMMAIRE

Ce que vous allez lire dans les 12 prochaines minutes.

01 **Pourquoi le cyber-risque rattrape les dirigeants en 2026** — p.3
Les quatre forces qui ont changé la nature du sujet.

02 **Pourquoi c'est devenu une décision de dirigeant** — p.5
Le sens business du sujet cyber, en quatre questions.

03 **Ce que votre police couvre, ce qu'elle ne couvre presque jamais** — p.6
Lecture détaillée des cinq briques d'une police cyber.

04 **Trois cas réels chiffrés du marché français** — p.8
Sopra Steria, Pierre Fabre, panel PME — et l'enseignement.

05 **Cinq questions à poser à votre assureur** — p.9
Celles qui décident de votre prime et de votre éligibilité.

06 **La méthode CLARTÉ CYBER — maîtrisé en 10 jours** — p.11
Huit étapes, un livrable opposable à toutes vos parties prenantes.

NOTE SUR LA MÉTHODE

Les données et benchmarks utilisés dans ce livre blanc proviennent de sources publiques et professionnelles : CESIN Baromètre 2025-2026, AMRAE LUCY 2025, ANSSI Panorama Cybermenace 2024, Hiscox Cyber Readiness Report, CLUSIF, Cybermalveillance.gouv.fr. Les cas chiffrés sont issus de communiqués officiels d'entreprises et de rapports d'autorités. Les ordres de grandeur PME proviennent de missions de diagnostic conduites par OG IT Consulting en 2024-2026.

CHAPITRE 01

Pourquoi le cyber-risque rattrape les dirigeants en 2026.

Quatre forces convergent simultanément. Aucune, prise isolément, n'aurait suffi à transformer le sujet. Leur combinaison change la nature du problème — et la nature de la décision.

1. La cyberattaque coûte aujourd'hui bien plus que ce qu'elle détruit.

Sur les PME tech françaises de 50 à 500 salariés, le coût direct d'une attaque sérieuse se situe entre 100 000 et 300 000 euros. Mais sur les 18 mois qui suivent, le coût total observé atteint 2 à 3 fois ce montant : surprime d'assurance, contrats stratégiques renégociés, temps dirigeant mobilisé, salariés-clés qui partent. Le sinistre n'est plus l'événement, c'est le déclencheur.

2. L'assurance n'est plus un transfert de risque, c'est un examen.

Le marché de l'assurance cyber PME a basculé entre 2022 et 2024. Les questionnaires sont passés de 20 à 60 questions. Les conditions imposent désormais la double authentification, des sauvegardes testées, une détection sur les postes 24/7, un plan de continuité documenté. Un dossier PME sur deux est refusé ou conditionné au premier passage (AMRAE LUCY 2025). Le marché ne couvre plus le risque : il vérifie qu'il est maîtrisé en amont.

60%
PME DISPARAISSANT DANS LES 18 MOIS SUIVANT UNE ATTAQUE SÉRIEUSE

×3,2
HAUSSE MOYENNE DES PRIMES CYBER PME ENTRE 2022 ET 2026

78%
GRANDS COMPTES EXIGEANT UN AUDIT CYBER FOURNISSEUR EN 2026

3. Les donneurs d'ordre auditent leurs fournisseurs avant de signer.

Pendant longtemps, la cyber arrivait après la signature. Cette époque est terminée. Les grands groupes français, sous pression de NIS2, de leurs assureurs et de leurs propres audits internes, ont placé la cybersécurité en filtre amont du processus achat. 78 % des appels d'offres significatifs incluent désormais un questionnaire cyber, accompagné d'une demande de preuves documentaires. Sur le panel observé, 60 % des PME tech sollicitées en 2025 n'ont pas pu produire l'ensemble des preuves dans le délai. Résultat : disqualification à l'entrée, ou contrats stratégiques renégociés.

4. NIS2 transfère la responsabilité au dirigeant.

La directive NIS2, transposée en droit français via la loi REIA, place la responsabilité de la gestion du cyber-risque au niveau de l'équipe dirigeante. L'organe de direction approuve, supervise, se forme. Sa responsabilité civile peut être engagée en cas de manquement. Les sanctions peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les entités essentielles. C'est un changement de logique juridique aussi structurant que le RGPD l'a été pour la donnée.

CE QUE CELA SIGNIFIE POUR VOUS

Le cyber-risque ne se traite plus comme un sujet IT ponctuel. Il se traite comme une responsabilité de dirigeant, qui exige une lecture lucide, des arbitrages éclairés et un dossier de preuves opposable à toutes vos parties prenantes : assureurs, clients, conseil d'administration, régulateur.

LE DOUBLE PIÈGE QUI GUETTE LE DIRIGEANT TECH

Premier piège : penser que le sujet est encore IT. Faux — la responsabilité est dirigeante, le coût est business, l'audit est commercial. Second piège : penser que le sujet attend. Faux — chacune des quatre forces est déjà active sur le marché français en 2026. Le renouvellement, l'appel d'offres, l'incident ou le contrôle se produisent quand ils se produisent. Aucun ne vous attend.

CHAPITRE 02

Pourquoi c'est devenu une décision de dirigeant.

Le cyber-risque n'est plus un sujet technique à arbitrer entre votre DSI et votre prestataire. C'est devenu une décision business qui engage votre marge, votre crédibilité commerciale, votre éligibilité aux marchés enterprise et votre propre responsabilité. Voici pourquoi, en quatre questions.

Pourquoi le cyber est-il devenu un sujet de comité de direction ?

Trois bascules structurelles l'expliquent. La première est financière : un sinistre cyber a aujourd'hui un impact direct sur l'EBITDA, sur la prime d'assurance et sur les arbitrages bilanciels. La deuxième est commerciale : un client enterprise qui suspend un contrat parce que vous ne passez plus son audit fournisseur, c'est un sujet de comité commercial, pas un sujet de DSI. La troisième est juridique : NIS2 a explicitement nommé l'organe de direction comme responsable. Aucune de ces trois bascules ne se règle au niveau de l'IT.

Pourquoi une PME tech doit-elle souscrire une assurance cyber ?

Pour quatre raisons cumulatives. Indemnisation : couvrir le coût direct d'un sinistre que vous ne pouvez pas auto-assurer. Posture client : un nombre croissant de grands donneurs d'ordre exigent une attestation d'assurance cyber dans leur process achat. Exigence régulatoire : pour certains secteurs et tailles, l'absence d'assurance devient un facteur aggravant en cas de contrôle. Signal aux investisseurs : un fonds qui regarde votre dossier en levée ou en exit demandera systématiquement votre dispositif d'assurance et de gestion de risque cyber.

Pourquoi évaluer le cyber-risque en amont coûte moins que le subir ?

Parce que le coût d'évaluation et de remédiation préventive est largement inférieur au coût de gestion post-sinistre, dans un rapport observé de 1 à 5, voire 1 à 10. Un diagnostic structuré coûte quelques milliers d'euros et débloque trois choses : la baisse de prime au renouvellement, l'évitement des contrats perdus, et la dispense de plans d'urgence en mode panique. À cela s'ajoute le temps dirigeant mobilisé en gestion de crise sur 9 à 12 mois, rarement modélisé, alors qu'il coûte plus cher que toutes les autres lignes additionnées.

Ce que font les acteurs existants, et ce qu'ils ne font pas.

Le DSI et le prestataire IT installent, configurent, exploitent. Ils ne décident pas du niveau de risque résiduel acceptable, ce n'est pas leur rôle. Le courtier place une police et négocie. Il ne vous dit pas si votre dispositif technique tient face aux exigences de la police. L'avocat sécurise vos contrats et votre conformité. Il ne vous donne pas la lecture économique de votre exposition réelle. Chacun fait bien sa partie ; personne ne fait l'arbitrage d'ensemble. Or c'est exactement l'arbitrage qui est demandé au dirigeant.

POURQUOI MAINTENANT, ET PAS DANS DEUX ANS

Parce que les quatre forces décrites au chapitre 01 sont déjà actives. Votre prochain renouvellement d'assurance, votre prochain audit client, votre prochain contrôle, ou votre prochain incident peuvent se produire dans les douze prochains mois. Aucun ne vous attend. Le coût d'un cyber-risque mal maîtrisé en 2026 n'est plus celui d'une attaque ; c'est celui de toutes les portes qui se ferment pendant que vous gérez la crise.

CHAPITRE 03

Ce que votre police couvre — et ce qu'elle ne couvre presque jamais.

Une police cyber standard pour PME tech ou SaaS se présente comme un produit unique. Dans les faits, elle se compose de cinq briques distinctes dont peu fonctionnent réellement sans condition. Voici le détail, brique par brique.

BRIQUE DE LA POLICE	CE QUI EST INCLUS	CE QUI EST EXCLU OU CONDITIONNÉ
Frais de gestion d'incident	Hotline 24/7, expert forensique, communication de crise, notification CNIL.	Plafonds rapidement atteints, souvent capés à 50-150 k€ — bien en deçà du coût réel observé.
Pertes d'exploitation	Perte de marge brute pendant l'arrêt d'activité.	Franchise temporelle (24-72 h) avant déclenchement ; durée d'indemnisation plafonnée.
Cyber-rançon	Prise en charge possible de la rançon et de la négociation.	Souvent exclue ou fortement conditionnée ; preuve de sauvegardes testées exigée.
Responsabilité civile	Dommages causés à des tiers (clients, partenaires) après fuite de données.	Exclusions pour faute de gestion ou non-conformité aux mesures déclarées.
Reconstruction des données	Frais de restauration des systèmes et des données.	Conditionnée à l'existence de sauvegardes conformes ; pertes contractuelles non couvertes.

LE MÉCANISME DE L'EXCLUSION-CLÉ

La majorité des refus d'indemnisation reposent sur une seule clause : la non-conformité de l'assuré aux mesures qu'il a lui-même déclarées dans le questionnaire de souscription. Si vous avez coché « MFA généralisée » et que l'attaque exploite un compte sans MFA, l'assureur invoque le manquement et limite ou refuse l'indemnisation. La preuve qui sauve, ce sont les logs et le journal de test.

Les trois exclusions qui transforment une police en faux ami.

Exclusion 1 — La faute de gestion.

Si votre dispositif déclaré n'est pas réellement appliqué — un EDR installé mais non maintenu, une sauvegarde jamais testée, une double authentification incomplète —, l'assureur peut invoquer la fausse déclaration et réduire l'indemnisation. La preuve qui sauve, ce n'est pas la conviction, ce sont les logs et le journal de test.

Exclusion 2 — La perte de contrats.

Lorsque vous perdez un client après un incident — qu'il vous notifie une rupture ou refuse de renouveler —, la perte commerciale n'est généralement pas couverte. Or c'est la première ligne de coût observée à 18 mois sur les PME tech. La police vous indemnise pour la reconstruction, pas pour la confiance perdue.

Exclusion 3 — Les dommages réputationnels long terme.

Les frais de communication de crise sont couverts. Le coût réel se matérialise plus tard : appels d'offres qui s'éloignent, prospects qui temporisent, recrutements qui patinent. Des coûts indirects qui s'étalent sur 6 à 18 mois, jamais modélisés en avance, ni pris en charge par la police.

LE BON RÉFLEXE

Ne lisez pas votre police comme un produit. Lisez-la comme un contrat de preuve. Pour chaque garantie, posez trois questions : que faut-il déclarer ? qu'est-ce qui sera vérifié en sinistre ? est-ce que je peux produire la preuve aujourd'hui ? Si la réponse à la troisième est non, vous êtes dans une zone d'exposition que la police ne couvrira pas.

CHAPITRE 04

Trois cas réels chiffrés du marché français.

Trois références publiquement documentées : deux grands groupes qui ont communiqué leur coût, et un panel de PME. Pour chacun, une seule chose à retenir.

Sources : communiqué AMF Sopra Steria (26/11/2020) · Le Monde, Bleeping Computer, ANSSI (Pierre Fabre) · AMRAE LUCY 2025 & CESIN 2025-2026 (panel PME).

40–50 M€
IMPACT SUR LE RÉSULTAT OPÉRATIONNEL

Cas 1 · Sopra Steria — Ransomware Ryuk (2020)

ESN de 46 000 collaborateurs. Plusieurs semaines pour tout rétablir. Rançon non payée.

La leçon : ce qui coûte, c'est la perte d'exploitation et les engagements contractuels — pas la rançon.

25 M$
RANÇON EXIGÉE, REFUSÉE

Cas 2 · Pierre Fabre — Ransomware Conti (2021)

Laboratoire pharma de 9 600 collaborateurs. Données exfiltrées et publiées, production perturbée.

La leçon : refuser de payer n'est tenable que si la résilience est construite en amont — sauvegardes testées, plan de continuité.

×2 à 3,5
COÛT DIRECT VS COÛT À 18 MOIS

Cas 3 · Panel PME français — AMRAE LUCY 2025

PME de 50 à 500 salariés sinistrées entre 2023 et 2025. Coût direct médian : 100 à 300 k€.

La leçon : votre police ne couvre qu'une fraction du coût réel. La vraie protection se joue en amont.

Ce que ces trois cas disent en commun

- **Le coût direct n'est que la partie visible.** Le coût réel se révèle sur 18 mois.
- **La résilience préalable fait la différence.** Elle sépare ceux qui sortent vite de ceux qui restent en crise des mois.
- **La part non indemnisée est devenue la règle,** pas l'exception : votre police ne vous couvrira pas pour tout.

82%
DU COÛT RÉEL D'UN SINISTRE N'EST PAS INDEMNISÉ EN MOYENNE

×2-3,5
MULTIPLICATEUR OBSERVÉ ENTRE COÛT DIRECT ET COÛT À 18 MOIS

9-12
MOIS DE MOBILISATION DIRIGEANTE POST-SINISTRE OBSERVÉE

CHAPITRE 05

Cinq questions à poser à votre assureur.

Au-delà du remplissage administratif, ce sont les cinq questions qui décident de votre prime, de vos franchises et de votre éligibilité même. Posez-les avant la signature. Posez-les au renouvellement. Et surtout, posez-les si vous pensez ne pas en avoir besoin.

01	La double authentification est-elle active sur 100 % des accès distants et sur tous les comptes à privilèges, sans exception ?
02	Pouvez-vous fournir un test de restauration de vos sauvegardes daté de moins de 6 mois, sur un système hors-ligne du périmètre principal ?
03	Disposez-vous d'un outil de détection sur les postes (type EDR) couvrant 100 % du parc, avec un service de supervision ?
04	Avez-vous un plan de continuité et de reprise d'activité documenté, daté, et testé au moins une fois dans les 12 derniers mois ?
05	Tenez-vous un registre de vos fournisseurs critiques et de leur niveau de sécurité, opposable en cas d'incident sur la chaîne ?

LE BON RÉFLEXE

Pour chacune de ces cinq questions, votre objectif n'est pas seulement de répondre oui — c'est de pouvoir produire la preuve. Un assureur qui doute en sinistre demandera systématiquement les éléments factuels : logs d'authentification, journal de test de sauvegarde, taux de couverture EDR, document de continuité daté, registre fournisseurs. C'est la preuve qui assure, pas la conviction.

Avant la souscription.

Posez ces 5 questions par écrit à votre courtier. Demandez les réponses par écrit également. Vous transformez la souscription en exercice de transparence : sur les points où vous êtes faibles, vous le savez et vous arbitrez. Sur les points où vous êtes forts, vous le documentez et vous obtenez une meilleure prime.

LE PIÈGE DU QUESTIONNAIRE OPTIMISTE

Sous la pression du temps et la peur du refus, beaucoup de dirigeants ou de responsables IT remplissent les questionnaires en surestimant le niveau réel de maîtrise. C'est de bonne foi, mais c'est la première cause des refus d'indemnisation. Mieux vaut une déclaration prudente que l'on tient, qu'une déclaration ambitieuse que l'on ne pourra pas démontrer en sinistre.

PROMESSE DE LA MÉTHODE

En 10 jours ouvrés, nous transformons une PME tech, un éditeur SaaS ou une ESN en organisation capable de répondre à toutes ses parties prenantes : assureurs, donneurs d'ordre, conseil d'administration, régulateur. Sans projet pluriannuel, sans rupture opérationnelle. Première brique de notre Programme de CyberConfiance & CyberAssurance.

CHAPITRE 06

La méthode CLARTÉ CYBER — maîtrisé en 10 jours.

CLARTÉ CYBER est la première brique de notre Programme de CyberConfiance & CyberAssurance (PCC). Huit étapes structurées sur dix jours ouvrés. Un seul livrable consolidé : le Dossier CLARTÉ, opposable à vos assureurs, à vos clients audit, à votre conseil et à votre responsabilité dirigeante.

01 JOUR 1

Kick-off stratégique

Cadrage de la mission, identification des actifs et processus critiques, validation du périmètre, première liste de risques perçus, analyse des dépendances IT et OT. Sortie : cadrage validé.

02 JOURS 2-3

Cartographie business et technique

Identification des données, systèmes, contrats, fournisseurs qui portent réellement votre activité. Lecture des polices et des contrats clients. Sortie : cartographie consolidée.

03 JOURS 4-5

Diagnostic des quatre leviers

Lecture lucide sur cybersécurité, gouvernance, assurance, résilience. Entretiens dirigeants et techniques. Test rapide des mesures critiques. Sortie : matrice d'exposition réelle vs perçue.

04 JOUR 6

Construction du score d'exposition

Agrégation en un score unique et lisible. Comparaison aux référentiels de marché (CESIN, AMRAE). Identification des trois écarts qui pèsent le plus sur votre prime. Sortie : score d'exposition daté.

05 JOUR 7

Plan d'actions priorisé sur 24 mois

Trois horizons : 3, 12 et 24 mois. Chaque action est associée à un coût, un risque résiduel et un livrable attendu. Sortie : roadmap chiffrée et priorisée.

06 JOUR 8

Dossier de preuves opposable

Constitution structurée : politiques, registres, tests, attestations. Format aligné avec les exigences assureur, audit client et NIS2. Sortie : dossier de preuves daté et signé.

07 JOUR 9

Préparation du dossier d'assurance

Mise en forme du dossier de souscription ou de renouvellement. Anticipation des questions sensibles, accompagnement face au courtier. Sortie : dossier d'assurance prêt à soumettre.

08
JOUR 10

Restitution dirigeante et conseil

Restitution synthétique au comité de direction ou au conseil. Trois choix structurants, conséquences chiffrées, recommandation argumentée. Sortie : trois décisions formalisées.

LE LIVRABLE UNIQUE

Le Dossier CLARTÉ est un livrable consolidé en un seul document : synthèse exécutive en 5 pages pour le conseil, plan d'actions chiffré sur 24 mois pour votre équipe, dossier de preuves structuré pour vos parties prenantes, et score d'exposition daté qui devient votre repère stable. Tout ce que vous devez avoir pour décider, pour prouver, pour négocier.

Délai : 10 jours ouvrés. **Mobilisation : ~10 heures cumulées de votre côté.** **Format : 100 % à distance ou hybride.**

• **SANS ENGAGEMENT**

15 minutes pour cadrer votre exposition.

Un échange court, structuré, sans engagement. Vous repartez avec une première lecture de votre exposition réelle et des trois écarts qui pèsent le plus sur votre assurabilité.

RÉSERVER MON CRÉNEAU DE 15 MIN

radia.ouro-gbele@og-it-consulting.com · og-it-consulting.com