OG IT CONSULTING

LIVRE BLANC · 2026

PROGRAMME CYBERCONFIANCE & CYBERASSURANCE

Cyber-Assurance PME : ce que votre police couvre vraiment. — et ce que vous risquez de découvrir trop tard.

Le guide stratégique des dirigeants de PME Tech, SaaS et ESN pour devenir réellement assurables, sécuriser leur crédibilité face aux clients enterprise, et reprendre la main sur leur exposition cyber.

ÉDITION TECH · SAAS · ESN

AUTEURE
Radia OURO-GBELE
Founder & Managing Director · OG IT Consulting

ÉDITION MAI 2026
OG-IT-CONSULTING.COM

ÉDITO

La cyber-assurance n'est plus un filet de sécurité. C'est un examen.

> En 2026, ce ne sont plus seulement les attaquants qui frappent vos systèmes. Ce sont aussi les assureurs qui durcissent leurs questionnaires, vos donneurs d'ordre qui exigent des preuves, et la directive NIS2 qui transfère la responsabilité jusqu'au comité de direction.

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, plus d' **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 auprès des clients enterprise 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 que nous appliquons en 10 jours pour rendre une PME Tech, SaaS ou ESN réellement assurable.

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

SOMMAIRE

Ce que vous allez lire dans les 8 prochaines minutes.

NOTE SUR LA MÉTHODE

Les chiffres et benchmarks utilisés dans ce livre blanc proviennent de l'expérience cumulée des consultants OG IT Consulting (CAC 40, ETI internationales, plus de 100 audits cybersécurité exécutés) et des données publiques 2024–2026 (ANSSI, ENISA, Cybermalveillance, Hiscox Cyber Readiness Report, sinistralité publiée par les principaux courtiers européens).

CHAPITRE 01

Pourquoi la cyber-assurance bascule en 2026 pour les PME Tech, SaaS et ESN.

> Quatre forces convergent simultanément. Aucune, prise isolément, n'aurait suffi. Mais leur combinaison rebat les cartes pour tout dirigeant Tech, SaaS ou ESN.

1. La sinistralité des PME a rattrapé celle des grands groupes.

Les attaquants ont changé de cible. Les grandes entreprises ont durci leurs défenses ; les PME Tech, elles, opèrent souvent en ouverture maximale (intégrations clients, multi-tenant, accès tiers) sans avoir formalisé leur dispositif de sécurité. Résultat : la PME Tech française est aujourd'hui aussi exposée — proportionnellement à son chiffre d'affaires — que ne l'était une ETI il y a cinq ans.

2. Les assureurs ont durci la souscription.

Le questionnaire de souscription est devenu un véritable audit. MFA généralisée, sauvegardes immuables, EDR, plan de réponse à incident, sensibilisation collaborateurs : en l'absence de preuves, le dossier est refusé, surprimé ou conditionné à des exclusions de garantie qui réduisent la couverture réelle à une fraction de la promesse commerciale initiale.

52 %	×3,2	1/2
PME AYANT SUBI UNE CYBERATTAQUE EN 2024-25	HAUSSE MOYENNE DES PRIMES CYBER 2022-2026	DOSSIERS PME REFUSÉS OU CONDITIONNÉS

3. NIS2 transfère la responsabilité au dirigeant.

La directive NIS2, désormais transposée et appliquée aux fournisseurs de services numériques, rend le dirigeant **personnellement responsable** de l'adéquation des mesures de cybersécurité. La sanction n'est plus seulement réputationnelle ou financière pour la société : elle remonte au niveau du mandataire social. Aucun assureur n'accepte de couvrir une faute personnelle de gouvernance.

4. Les donneurs d'ordre exigent des preuves contractuelles.

Vos clients enterprise — grands comptes industriels, banques, assureurs, retailers — exigent désormais des questionnaires sécurité de plus en plus longs avant chaque signature. Ne pas pouvoir y répondre proprement, c'est **perdre des appels d'offres** avant même de les avoir disputés.

CE QUE CELA SIGNIFIE POUR VOUS

La cyber-assurance n'est plus un produit que l'on achète : c'est un statut que l'on mérite. Et ce statut conditionne désormais à la fois votre capacité à signer des contrats et votre capacité à dormir tranquille en tant que dirigeant.

Le secteur Tech est sous tension marché croissante.

Sur les missions de diagnostic conduites en 2024-2026 auprès de PME Tech, SaaS et ESN françaises, **71 % des dirigeants pensaient être correctement assurés** . Après analyse de leur police et de leur exposition réelle, seuls 18 % l'étaient véritablement. L'écart se situe presque toujours au même endroit : la perte d'exploitation et les exclusions liées à la non-conformité.

LE DOUBLE PIÈGE QUI GUETTE LE DIRIGEANT TECH

Piège 1 — La fausse sécurité. Vous payez une prime élevée, vous pensez avoir transféré le risque. En réalité, votre police comporte des exclusions qui ne se révèlent qu'au moment où un client enterprise vous demande l'attestation post-incident. Piège 2 — Le refus silencieux. Vous demandez un renouvellement, l'assureur exige un questionnaire approfondi, vous êtes refusé. Désormais, votre dossier est marqué auprès du réseau de courtiers — et de vos clients enterprise les plus exigeants.

CHAPITRE 02

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 trois briques distinctes — dont une seule fonctionne réellement sans condition.

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.
Pertes d'exploitation	Perte de marge brute pendant l'arrêt d'activité.	Franchise temporelle (24–72 h). Exclusion en cas de non-conformité aux mesures déclarées.
Rançon (extorsion)	Paiement de la rançon dans certains pays.	Interdit ou très restreint en France. Sous-limite quasi systématique.
Reconstitution de données	Restauration depuis sauvegardes, reconstitution forensique.	Exclusion si les sauvegardes ne sont pas isolées (immuables / offline).
Responsabilité civile cyber	Mise en cause par tiers (clients, partenaires).	Exclusion en cas de faute lourde de gestion ou défaut de mesures déclarées.
Pénalités contractuelles	Très rarement inclus.	Quasi toujours exclu. C'est pourtant ici que se loge le plus gros coût d'un sinistre.

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.

CHAPITRE 02 · SUITE

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 existante mais non testée — l'assureur peut requalifier le sinistre en faute de gestion. Cette exclusion mord d'autant plus dur en contexte NIS2, où la responsabilité du dirigeant est explicitement engagée.

Exclusion 2 — La perte de contrats.

Lorsque vous perdez un client après un incident — soit parce qu'il vous a notifié une rupture, soit parce qu'il a fait jouer une clause de réversibilité — la prime cyber ne couvre presque jamais ce manque à gagner. Or sur les missions que nous conduisons, c'est la première source de perte économique post-incident pour une PME Tech ou SaaS.

Exclusion 3 — Les dommages réputationnels long terme.

Les frais de communication de crise sont couverts, mais le coût réel se matérialise plus tard : appels d'offres remportés en moins, conditions commerciales durcies, rallongement du cycle de vente. Aucune police standard ne le compense.

> **LE BON RÉFLEXE**
> Ne lisez pas votre police comme un produit. Lisez-la comme un **contrat conditionnel** : chaque garantie est suspendue à un engagement de votre part, et chaque engagement est testé au moment du sinistre. La meilleure assurance n'est pas celle qui promet le plus : c'est celle dont vous êtes en mesure de tenir tous les engagements.

Le bon ordre de marche.

Trop de PME Tech et SaaS abordent la cyber-assurance comme un produit à acheter. Le bon ordre est l'inverse : **évaluer son exposition réelle, mettre en conformité ses mesures déclarables, puis négocier son assurance** en position de force. C'est précisément la trajectoire que la méthode CLARTÉ CYBER déroule en 10 jours.

CHAPITRE 03

Le gap réel entre votre risque et votre couverture, en chiffres.

Les trois scénarios qui suivent sont tirés de cas réels rencontrés sur le segment PME Tech, SaaS et ESN françaises (CA 10–80 M€), anonymisés. Ils illustrent un mécanisme central : la perte économique réelle est presque systématiquement supérieure à l'indemnisation reçue.

Scénario 1 · Ransomware sur éditeur SaaS B2B (CA 22 M€)

TECH SAAS

Compromission via un compte d'admin partenaire sans MFA, chiffrement de l'environnement de production. Service indisponible pour les clients enterprise pendant 11 jours.

COÛT ÉCONOMIQUE RÉEL
2 850 000 €
- ✗ Perte d'exploitation (11 j) — 1,4 M€
- ✗ Pénalités SLA contrats enterprise — 480 k€
- ✗ Forensique & remédiation — 220 k€
- ✗ Churn de 2 clients enterprise — 750 k€

INDEMNISATION EFFECTIVE
510 000 €
- ✓ Frais de gestion (plafond) — 150 k€
- ✓ Perte d'expl. (franchise 72h, sous-limite) — 360 k€
- ✓ Pénalités & pertes contrats — non couvert

RESTE À CHARGE DIRIGEANT **2 340 000 €**

Scénario 2 · Fraude au virement par compromission email (CA 14 M€)

TECH SAAS

Compromission de la boîte mail du DAF, modification d'un IBAN fournisseur, virement détourné de 380 k€. Détection à J+9.

COÛT ÉCONOMIQUE RÉEL
490 000 €
- ✗ Virement détourné — 380 k€
- ✗ Frais juridiques & expertise — 65 k€
- ✗ Reconstruction confiance fournisseur — 45 k€

INDEMNISATION EFFECTIVE
75 000 €
- ✓ Sous-limite « fraude au président » plafonnée
- ✓ Exclusion partielle : défaut de double validation déclaré

RESTE À CHARGE DIRIGEANT **415 000 €**

CHAPITRE 03 · SUITE

Le scénario que personne ne voit venir : le refus de souscription.

Scénario 3 · Refus de souscription après audit assureur (CA 38 M€)

TECH SAAS

Éditeur SaaS B2B en levée série B. Un grand compte enterprise exige une attestation cyber-assurance + ISO 27001 dans les 6 mois. Refus des trois assureurs sollicités après questionnaire approfondi : MFA partielle, sauvegardes non immuables, absence de plan de réponse formalisé.

COÛT ÉCONOMIQUE RÉEL
1 200 000 €
✗ Perte de l'appel d'offres concerné — 800 k€
✗ Conditions durcies sur 2 contrats existants — 280 k€
✗ Mise en place urgence en 4 mois — 120 k€

INDEMNISATION EFFECTIVE
0 €
✓ Aucune police active
✓ Le refus n'est pas un sinistre — aucune protection

RESTE À CHARGE DIRIGEANT **1 200 000 €**

Ce que ces scénarios disent en commun.

Trois patterns ressortent systématiquement : **(1)** la franchise et les sous-limites annulent une grande partie de la promesse commerciale, **(2)** les exclusions liées à la non-conformité aux mesures déclarées s'activent au pire moment, **(3)** les pertes les plus lourdes — contrats, pénalités, réputation — ne sont presque jamais couvertes.

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

10 j
POUR PASSER DE « NON ASSURABLE » À « ASSURABLE ET NÉGOCIÉ »

3-5 ×
ROI MOYEN D'UN PROGRAMME PCC SUR 24 MOIS

CHAPITRE 04

Cinq questions qui changent toute négociation avec un assureur.

> Posez-les avant la signature. Posez-les au renouvellement. Posez-les surtout si vous pensez ne pas en avoir besoin : c'est précisément à ce moment-là qu'elles sont les plus utiles.

01 **Quelles sont précisément les exclusions liées à la non-conformité de mes mesures déclarées ?**

Faites lister, en clauses opposables, ce que l'assureur considère comme un manquement matériel. Demandez la définition exacte de « MFA généralisée », « sauvegardes immuables », « plan de réponse à incident ».

02 **Quelle est la franchise temporelle de la perte d'exploitation, et que couvre-t-elle vraiment ?**

72 heures de franchise excluent la majorité des incidents PME. Demandez à voir un exemple de calcul d'indemnisation sur un sinistre type, avec les sous-limites par poste.

03 **Les pénalités contractuelles et la perte de contrats sont-elles couvertes ?**

Quasi toujours exclues. Si elles sont mentionnées, faites-les chiffrer en sous-limite et vérifiez les conditions d'activation. C'est le poste où vos pertes seront les plus lourdes.

04 **Comment est traitée la responsabilité personnelle du dirigeant au regard de NIS2 ?**

Demandez explicitement si une condamnation au titre de NIS2 entraîne une exclusion. La plupart des polices ne couvrent pas la faute personnelle de gouvernance — c'est un angle mort majeur.

05 **En cas de sinistre, quel est le délai entre la déclaration et le premier acompte ?**

Un sinistre cyber, c'est de la trésorerie qui brûle vite. Exigez un engagement contractuel sur un acompte en J+10 et un règlement final clair.

CHAPITRE 04 · SUITE

Comment les utiliser concrètement.

Avant la souscription.

Posez ces 5 questions par écrit à votre courtier. Demandez les réponses par écrit également. Vous transformez un échange commercial en élément contractuel opposable, et vous identifiez immédiatement les courtiers et assureurs sérieux des autres.

Pendant la négociation.

Utilisez ces réponses pour comparer les offres. Le critère ne doit jamais être uniquement le montant de la prime ou le plafond annoncé : c'est **la couverture réelle nette d'exclusions** , calculée scénario par scénario.

Au renouvellement.

Sortez le questionnaire de l'année précédente. Comparez ligne par ligne avec votre situation actuelle. Toute déclaration imprécise ou caduque est un risque d'exclusion futur. C'est exactement ce que les assureurs recherchent désormais.

> **LE PIÈGE DU QUESTIONNAIRE OPTIMISTE**
> Sous la pression du temps et la peur du refus, beaucoup de dirigeants — ou leurs DSI — cochent par optimisme des cases qui ne correspondent pas à la réalité opérationnelle. Cette pratique est l'une des principales causes de refus d'indemnisation post-sinistre. Mieux vaut un dossier sincère et progressif qu'une attestation séduisante mais juridiquement fragile.

L'étape suivante : passer du diagnostic à l'éligibilité.

Si ces questions vous mettent dans une position inconfortable — c'est sain : c'est la première étape de la lucidité stratégique. La seconde consiste à transformer cette lucidité en plan d'action mesurable. C'est précisément le rôle de la méthode CLARTÉ CYBER, dans le cadre de notre Programme de CyberConfiance & CyberAssurance (PCC).

> **PROMESSE DE LA MÉTHODE**
> En 10 jours ouvrés, nous transformons une PME Tech, SaaS ou ESN non éligible (ou éligible aux mauvaises conditions) en candidate **réellement assurable et défendable** auprès des principaux courtiers européens.

CHAPITRE 05

La méthode CLARTÉ CYBER — devenir assurable en 10 jours.

CLARTÉ CYBER est la première brique de notre Programme de CyberConfiance & CyberAssurance (PCC). 8 étapes, 10 jours ouvrés, et un livrable unique : votre Passeport Cybersécurité & Éligibilité Cyberassurance — calibré sur les attentes des clients enterprise et investisseurs.

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/OT.

Sortie : cadrage validé

02 JOURS 2-3

Diagnostic et entretiens

Entretiens avec direction, IT, métiers et finance. État de la gouvernance des données, accès admin et MFA, infrastructure, historique d'incidents, niveau d'assurance actuel.

Sortie : vision claire de l'exposition

03 JOURS 4-5

Analyse des risques

Construction de 8 à 12 scénarios d'attaques contextualisés (ransomware, fraude email, attaque OT, supply chain). Évaluation impact business, probabilité, niveau de maîtrise et priorité.

Sortie : cartographie des risques + impacts

04 JOUR 6

BIA — Business Impact Analysis

Atelier de 2 heures avec votre équipe pour mesurer l'impact business réel d'une attaque cyber. Analyse approfondie de 5 à 8 processus critiques.

Sortie : chiffrage de votre exposition réelle

CHAPITRE 05 · SUITE

De l'analyse à la signature de votre cyber-assurance.

05 JOUR 7

ROI sécurité

Estimation chiffrée de vos pertes potentielles. Proposition d'une priorisation des investissements de sécurité, alignée sur votre exposition réelle et votre capacité de financement.

Sortie : arbitrage risques / investissements

06 JOUR 8

Roadmap 24 mois

Plan d'action priorisé sur 24 mois, articulé par trimestres. Évaluation des dépendances, estimation budgétaire, cadrage RH et choix des prestataires.

Sortie : roadmap claire et défendable

07 JOUR 9

Cyber-Assurance Readiness

Pré-remplissage des questionnaires assureurs, organisation des preuves, structuration du dossier de souscription, coordination avec les courtiers de notre réseau partenaire.

Sortie : dossier d'éligibilité complet

08 JOUR 10

Restitution exécutive

Synthèse devant la direction, validation de la roadmap, mise en relation avec les courtiers sélectionnés, remise du Passeport Cybersécurité.

Sortie : Passeport CyberAssurance

LE LIVRABLE UNIQUE

Le Passeport Cybersécurité & Éligibilité Cyberassurance est un dossier exécutif que vous pouvez présenter à votre comité de direction, à vos donneurs d'ordre et à vos courtiers. Il vous donne, en une seule pièce, une vision claire de vos risques, une trajectoire crédible sur 24 mois et un statut d'éligibilité documenté auprès des principaux assureurs cyber européens.

Tarif : 12 000 € HT, forfaitisé.
Délai : 10 jours ouvrés.
Mobilisation : En moyenne 10 h cumulées de votre équipe.
ROI documenté : 3 à 5× sur la 1re année.

PASSER À L'ACTION

15 minutes pour cadrer votre exposition. Et savoir si vous êtes réellement assurable.

Un échange court, structuré, sans engagement. Nous écoutons votre situation, nous identifions vos angles morts, et nous vous indiquons la meilleure trajectoire pour les 90 prochains jours — que vous travailliez avec nous ou non.

RÉSERVER MON CRÉNEAU DE 15 MIN

SANS ENGAGEMENT
Aucune obligation, aucune carte bancaire, aucun pitch commercial.

AVEC UN DIRIGEANT
L'échange se tient avec Radia ou un consultant senior — pas un commercial.

UNE VRAIE VALEUR
Vous repartez avec une lecture claire de vos 3 risques majeurs et de votre niveau d'assurabilité.

VOTRE INTERLOCUTRICE

Radia OURO-GBELE
Founder & Managing Director

CONTACT

contact@og-it-consulting.com
+33 6 69 50 78 02
Paris, France · og-it-consulting.com

OG IT CONSULTING