Cyber Assurance 2026 : Guide Souscription et Gestion des Sinistres

Guide cyber assurance 2026 — critères de souscription MFA/EDR, couvertures ransomware/BEC, questionnaires sécurité, sinistres et marché assureurs France.

Le marché de la cyber assurance en France a connu une transformation profonde entre 2020 et 2026. Après les années de sinistralité exceptionnelle liées à l'explosion des ransomwares (2020-2022), les assureurs ont drastiquement durci leurs critères de souscription, relevé les primes, renforcé les exclusions et rendu certaines couvertures conditionnelles à des niveaux de maturité cyber minimaux. En 2026, souscrire une cyber assurance efficace nécessite une préparation sérieuse et une compréhension des attentes des assureurs : MFA déployé sur tous les accès distants, EDR actif sur les endpoints, sauvegardes testées et isolées, gestion des vulnérabilités documentée. Sans ces prérequis, soit la police sera refusée, soit les exclusions rendront la couverture quasi-théorique lors d'un sinistre réel. Ce guide couvre l'ensemble du cycle de vie de la cyber assurance pour les entreprises françaises : compréhension du marché (AXA XL, Allianz Cyber, Hiscox, Beazley, SMABTP), critères de souscription en 2026, types de couvertures disponibles, lecture des conditions particulières et exclusions, questionnaires d'évaluation de la maturité cyber, procédures en cas de sinistre ransomware ou BEC, et perspectives du marché à horizon 2027. La cyber assurance n'est pas un substitut à la cybersécurité — c'est un filet de sécurité financier conditionné à une posture cyber sérieuse.

À RETENIR

À retenir — Cyber Assurance 2026

• **MFA obligatoire** sur tous les accès distants (VPN, RDP, email) : condition sine qua non de souscription en 2026

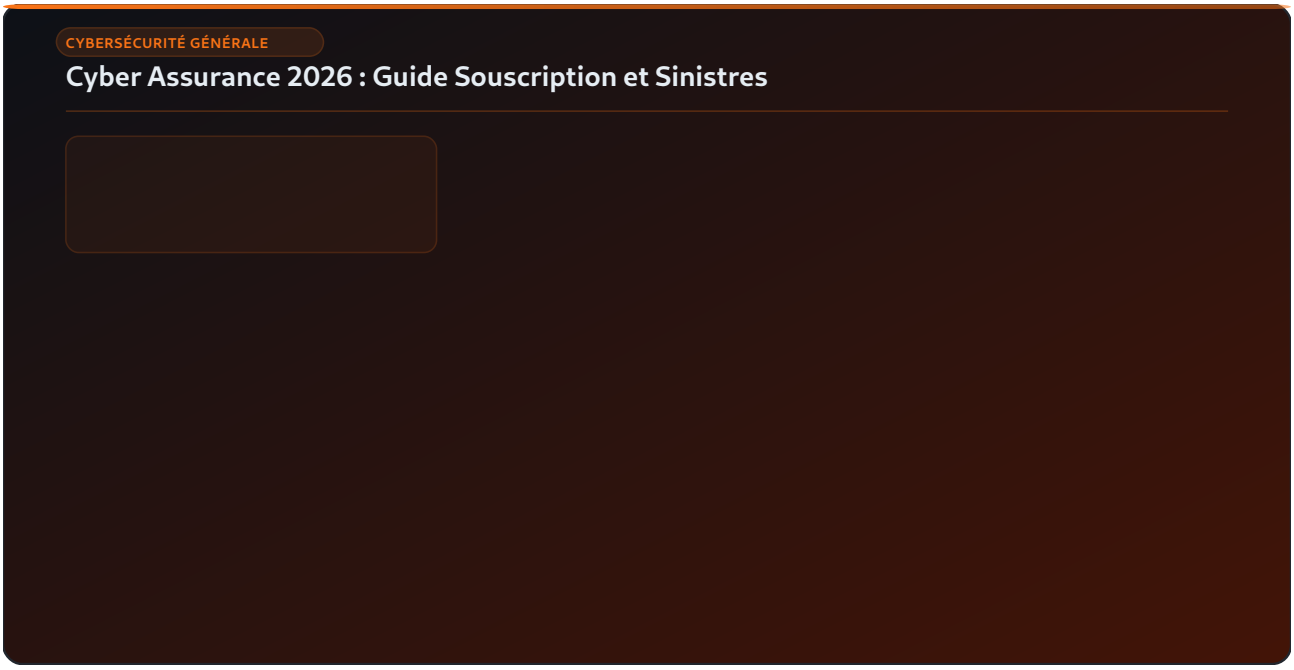
• **EDR déployé** sur 100% des endpoints : exigé par la majorité des assureurs principaux

• Sauvegardes **testées et isolées** (règle 3-2-1) : vérifiées lors du questionnaire et parfois lors d'audit

• Exclusions courantes à lire : guerre/cyberguerre, infrastructure nationale, amendes réglementaires

• En cas de sinistre ransomware : notifier l'assureur **avant** tout paiement de rançon

• Marché France 2026 : primes en baisse relative mais questionnaires plus exigeants



Le marché de la cyber assurance en France a atteint une relative maturité en 2026 après la tempête de la période 2020-2022. Les primes ont connu une hausse spectaculaire (+100 à +200% en 2021-2022) liée à une sinistralité ransomware exceptionnelle, avant de se stabiliser et de légèrement reculer en 2023-2025 sous l'effet de la concurrence accrue et de l'amélioration de la posture cyber des entreprises assurées. Les principaux assureurs actifs sur le marché français en

2026 incluent **AXA XL** (leader historique, offre complète), **Allianz Cyber** (forte présence PME/ETI), **Hiscox** (spécialiste cyber, questionnaire en ligne innovant), **Beazley** (spécialiste Lloyd's, fort en réponse à incident), **AIG CyberEdge**, **Chubb Cyber Enterprise Risk Management**, et pour les collectivités et établissements publics, **SMACL** et **SMABTP**. Le marché français représentait environ 400 millions d'euros de primes en 2025, en croissance de 15% par rapport à 2024, porté par la prise de conscience post-NIS 2 et les exigences des donneurs d'ordres envers leurs sous-traitants. La réassurance cyber — longtemps tendue — s'est légèrement détendue en 2025-2026, permettant aux assureurs primaires d'élargir leurs capacités.

Critères de souscription cyber 2026 : les prérequis incontournables

En 2026, les assureurs cyber ont convergé vers un ensemble de prérequis techniques dont l'absence entraîne soit un refus de couverture, soit des exclusions tellement larges que la police devient inefficace. Le premier prérequis est le **MFA (Multi-Factor Authentication)** sur tous les accès distants : VPN, RDP, webmail, portails administratifs. L'absence de MFA sur ces accès est le facteur de risque numéro un identifié lors des sinistres ransomware et BEC — les assureurs l'ont donc rendu obligatoire. Le deuxième prérequis est un **EDR (Endpoint Detection and Response)** déployé sur 100% des endpoints Windows et Mac, avec des alertes actives et des équipes capables d'y répondre. Un antivirus traditionnel n'est plus suffisant. Le troisième prérequis est la présence de **sauvegardes testées et isolées** : la règle 3-2-1 (3 copies, 2 médias différents, 1 hors-site) avec des tests de restauration documentés trimestriels. Le quatrième prérequis est une **gestion des vulnérabilités active** : scan régulier, processus de patch management documenté, délais de correction définis par criticité. Le cinquième, de plus en plus fréquent, est la **formation anti-phishing** avec simulation régulière et mesure du taux de clic.

⚡ **Retour terrain**

Dans mes missions d'audit, je rencontre régulièrement la même configuration à risque : des règles de firewall héritées depuis 5 à 10 ans, que personne n'ose supprimer par crainte de casser quelque chose. J'ai développé une méthode de nettoyage progressive — analyser les logs de connexion sur 90 jours, identifier les règles sans trafic, les désactiver sans supprimer pendant 30 jours, puis valider avec les équipes métier. Sur un parc de 340 règles dans un groupe logistique, nous en avons supprimé 218 sans incident.

Questionnaire de souscription cyber : ce que les assureurs évaluent réellement

Le questionnaire de souscription cyber est devenu le principal outil d'évaluation de la maturité cyber par les assureurs. En 2026, ces questionnaires ont évolué de simples check-lists vers de véritables évaluations techniques approfondies. Hiscox propose ainsi un questionnaire en ligne de 45 à 80 questions selon la taille de l'entreprise, couvrant les contrôles techniques et organisationnels. Les domaines évalués systématiquement incluent : les contrôles d'accès (MFA, PAM, gestion des comptes privilégiés) ; la gestion des endpoints (EDR, chiffrement des disques, politique BYOD) ; la protection email (SPF/DKIM/DMARC, filtrage anti-phishing, sandbox) ; les sauvegardes (fréquence, isolation, tests de restauration) ; la gestion des tiers (évaluation sécurité des fournisseurs critiques) ; le plan de réponse aux incidents (CSIRT interne ou externalisé, exercices annuels) ; et les données personnelles (cartographie RGPD, DPO désigné). Des questions spécifiques portent sur les **incidents passés** : avoir subi un ransomware ou une BEC sans le déclarer à l'assureur est une cause potentielle de nullité du contrat. La transparence est indispensable — les assureurs procèdent à des vérifications techniques post-souscription et pré-sinistre.

Types de couvertures cyber en 2026 : analyse détaillée

Une police de cyber assurance complète en 2026 couvre plusieurs volets distincts. La **réponse à incident** finance l'intervention d'une équipe CSIRT externe (retenue par l'assureur ou libre choix selon les polices), les investigations forensiques, la notification des victimes en cas de violation de données, et les frais de conseil juridique. La **perte d'exploitation** (Business Interruption) compense le chiffre d'affaires perdu pendant la période d'indisponibilité des systèmes — souvent le poste le plus important dans les sinistres ransomware, avec des délais de carence de 8 à 24 heures et des plafonds journaliers. La **couverture extorsion/ransomware** finance le paiement d'une rançon si la décision est prise (sous conditions) et les frais de négociation avec les extorqueurs. La **responsabilité civile cyber** couvre les dommages subis par des tiers (clients, partenaires) suite à un incident cyber dont l'assuré est responsable. La **cyber fraude** couvre les pertes liées aux virements frauduleux BEC/CEO fraud. Enfin, la **gestion de crise** couvre les frais de communication de crise et de RP post-incident. Ces couvertures s'accompagnent de franchises, sous-limites et conditions spécifiques qui nécessitent une lecture attentive des conditions particulières.

Exclusions cyber : les clauses qui vident les polices de leur substance

La lecture fine des exclusions est aussi importante que la lecture des garanties dans une police cyber. Les exclusions les plus impactantes en 2026 incluent la **clause guerre/cyberguerre** : depuis les attaques liées au conflit russo-ukrainien (NotPetya 2017, attaques bancaires ukrainiennes), les assureurs ont tenté d'élargir cette exclusion aux cyberattaques étatiques. Après des litiges majeurs (Mondelez vs Zurich, Merck vs ses assureurs), une définition plus précise a été négociée : les attaques étatiques ciblées sont exclues, les dommages collatéraux d'attaques non ciblées restent couverts. La **clause d'infrastructure nationale** exclut les dommages résultant d'attaques sur des infrastructures critiques (électricité, eau, télécoms) qui rendraient inopérables les systèmes de l'assuré. Les **amendes réglementaires** (RGPD, NIS 2, CNIL) ne sont généralement pas couvertes en France car contraires à l'ordre public. Les **dommages intentionnels** commis par des dirigeants de l'entreprise sont exclus. Les **vulnérabilités connues**

non patchées : certaines polices excluent les sinistres résultant d'une CVE publiée depuis plus de X jours sans avoir été corrigée — une exclusion très contestable mais présente chez certains assureurs.

Procédure de sinistre ransomware : les 72 premières heures

Lors d'un sinistre ransomware, les **72 premières heures** sont critiques à la fois pour la limitation des dégâts et pour la couverture assurantielle. La première action est la **notification immédiate de l'assureur** — avant toute décision de payer ou non la rançon, avant toute communication externe. La plupart des polices imposent une notification dans les 24 à 72 heures sous peine de déchéance de garantie. L'assureur met alors à disposition son prestataire CSIRT (ou valide votre prestataire si liberté de choix) pour l'investigation et la réponse à incident. La deuxième action est la **préservation des preuves** : ne pas éteindre les systèmes impactés brutalement, capturer des images mémoire si possible, documenter le périmètre de l'incident. La troisième action est la **notification CNIL** sous 72 heures si des données personnelles sont concernées — en parallèle, pas en remplacement, de la notification assureur. La quatrième action est la **décision sur le paiement de la rançon** : cette décision doit être prise en concertation avec l'assureur, le CSIRT, les avocats spécialisés et la direction. En France, payer une rançon n'est pas illégal en soi mais peut l'être si le groupe ransomware est sanctionné (liste OFAC américaine, sanctions européennes). Un retour terrain : lors d'un sinistre ransomware sur une PME industrielle française en 2025, la direction avait payé la rançon avant de notifier l'assureur — la compagnie a argué que l'absence de notification préalable constitue un manquement contractuel réduisant l'indemnisation de 40%.

Sinistre BEC (Business Email Compromise) : spécificités assurantielles

Les sinistres **BEC (Business Email Compromise)** — fraudes au virement impliquant usurpation d'identité par email — présentent des spécificités assurantielles importantes. La couverture BEC

est incluse dans la cyber fraude ou la cybercriminalité, selon la terminologie des polices. Les conditions de couverture incluent généralement : la preuve que l'adresse email source a bien été compromise (usurpation ou piratage), et non simplement imitée (adresse similaire sans piratage). Une fraude par email similaire mais non piraté peut relever de la garantie fraude générale et non cyber — une distinction importante avec des conséquences sur les franchises et les plafonds. Les **délais de déclaration** sont particulièrement critiques dans les BEC : le virement ayant souvent déjà été effectué, chaque heure compte pour tenter un recall bancaire (récupération du virement auprès de la banque destinataire). Les banques disposent d'un mécanisme de recall sous 24-48 heures avec des taux de récupération variables selon la juridiction du bénéficiaire. Les **plafonds BEC** sont souvent inférieurs aux plafonds ransomware dans les polices cyber — à vérifier lors de la souscription, notamment si l'exposition BEC est significative (entreprise avec des flux de paiements importants).

Couverture OT et systèmes industriels : un marché de niche

La couverture des **systèmes OT (Operational Technology)** dans les polices cyber est un domaine encore peu mature mais en rapide évolution. Les sinistres OT présentent des caractéristiques uniques : potentiel de dommages physiques (équipements endommagés par des commandes malveillantes), arrêts de production prolongés, et risques environnementaux ou pour la sécurité des personnes qui dépassent largement les simples pertes IT. La plupart des polices cyber standard n'incluent pas explicitement les systèmes OT ou prévoient des exclusions ou sous-limites spécifiques. Des assureurs comme Beazley, Hiscox et AXA XL proposent des extensions OT spécifiques, avec des questionnaires dédiés évaluant la segmentation IT/OT, la présence d'un monitoring OT (Claroty, Nozomi) et les plans de continuité industrielle. Pour les entreprises industrielles, la coordination entre la cyber assurance et l'assurance dommages aux biens (qui couvre traditionnellement les équipements physiques) est indispensable pour éviter les lacunes de couverture en cas d'incident cyber provoquant des dommages physiques. Des clauses de "cyber event" dans les polices IARD (Incendie, Accidents, Risques Divers) commencent à apparaître, mais leur rédaction reste hétérogène.

Audit de souscription cyber : comment se préparer

De plus en plus d'assureurs cyber complètent le questionnaire de souscription par un **audit technique** — une visite d'évaluation ou un scan externe de la surface d'attaque. Certains assureurs (Beazley, Hiscox) utilisent des outils d'évaluation de la posture cyber externe (BitSight, SecurityScorecard) pour scorer automatiquement le niveau de sécurité visible depuis Internet avant même la souscription. Un score BitSight inférieur à 650 ou un SecurityScorecard inférieur à C peut bloquer la souscription ou imposer une surprime. Pour préparer un audit ou améliorer son score externe : fermer les ports non nécessaires exposés sur Internet, corriger les vulnérabilités visibles depuis l'extérieur (Shodan, scan externe), mettre en place SPF/DKIM/DMARC sur les domaines email, et s'assurer que les certificats SSL/TLS sont valides et à jour. En interne, avoir une documentation claire de la politique de sécurité, des preuves de tests de sauvegardes récents, et des logs de déploiement MFA est indispensable pour répondre aux questions de l'auditeur. La préparation à l'audit cyber est souvent un accélérateur bienvenu pour des projets de sécurité qui stagnaient faute de budget — la perspective d'obtenir (ou de maintenir) une couverture cyber à un tarif raisonnable est un argument décisif auprès des directions financières.

Prime cyber en 2026 : facteurs de tarification et optimisation

La **prime d'assurance cyber** est calculée sur la base de plusieurs facteurs. Le **chiffre d'affaires** ou le bilan total reste la principale variable de base. Le **secteur d'activité** joue un rôle majeur : les secteurs de la santé, de la finance et de l'éducation sont considérés comme plus risqués et tarifiés plus cher. La **maturité cyber** évaluée par le questionnaire permet d'obtenir des réductions significatives : une entreprise avec MFA, EDR, sauvegardes testées et programme de sensibilisation obtient typiquement 20 à 40% de réduction par rapport à une entreprise équivalente sans ces contrôles. Le **capital assuré et les franchises** permettent d'ajuster la prime — une franchise élevée (100 000 € vs 10 000 €) réduit significativement la prime. Les **antécédents de sinistres** sont pris en compte : un sinistre déclaré dans les 3-5 ans passés majore la prime ou peut conduire à un refus. Pour optimiser la prime, plusieurs leviers sont disponibles :

démontrer la maturité cyber avec des preuves documentées (rapports de pentest, attestations PASSI, certificats ISO 27001), choisir une franchise adaptée au profil de risque réel, et faire jouer la concurrence entre assureurs via un courtier spécialisé.

Rôle du courtier cyber spécialisé

Le recours à un **courtier en assurance cyber spécialisé** est fortement recommandé pour les entreprises de plus de 50 salariés ou dont le chiffre d'affaires dépasse 10 millions d'euros. Le courtier apporte plusieurs valeurs ajoutées spécifiques au risque cyber. La **connaissance du marché** : il connaît les appétits des assureurs, leurs exclusions types et leurs tarifications, permettant de placer le risque auprès de l'assureur le mieux adapté au profil de l'entreprise. L'**assistance à la rédaction du questionnaire** : un questionnaire mal rempli peut conduire à une sous-couverture ou à un refus — le courtier aide à répondre de manière précise et favorable. La **comparaison des polices** au-delà de la prime : les différences entre polices cyber portent souvent sur des détails (définition du sinistre, liste des prestataires de réponse à incident mandatés, couverture internationale) qui n'apparaissent qu'à la lecture fine des conditions générales. L'**assistance en cas de sinistre** : le courtier est l'interlocuteur entre l'assuré et l'assureur lors du sinistre, facilitant la mise en œuvre de la couverture et défendant les intérêts de l'assuré. En France, des courtiers spécialisés cyber comme Siaci Saint Honoré, Marsh, Aon et Verspieren ont développé des équipes dédiées avec des compétences techniques en cybersécurité.

Cyber assurance et RGPD : articulation des obligations

L'articulation entre la cyber assurance et les obligations **RGPD** est un sujet complexe mais important pour toute entreprise traitant des données personnelles. Les frais de notification RGPD (information des personnes concernées, frais postaux, call center dédié) sont généralement couverts par les polices cyber dans le volet "gestion des incidents" ou "notification des tiers". La **couverture de la responsabilité civile RGPD** vis-à-vis des personnes dont les données ont été

compromises est incluse dans la responsabilité civile cyber. En revanche, les **amendes CNIL** ne sont pas assurables en France — l'ordre public s'y oppose. La consultation d'un **DPO (Data Protection Officer)** en amont de la souscription permet d'identifier les risques RGPD les plus significatifs (types de données traitées, volumes, transferts hors UE) et de s'assurer que la police cyber les couvre adéquatement. Une erreur fréquente : les polices cyber ne couvrent généralement pas les violations de données résultant d'une erreur humaine non malveillante (email envoyé au mauvais destinataire, fichier partagé publiquement par mégarde) — à vérifier car ces incidents représentent une part importante des notifications CNIL.

Cyber assurance pour TPE/PME : offres simplifiées

Le marché de la cyber assurance pour les TPE/PME a été longtemps sous-développé en France, les offres étant principalement conçues pour les grandes entreprises. En 2026, plusieurs acteurs proposent des offres simplifiées adaptées aux petites structures. **Hiscox Direct** propose un parcours de souscription en ligne en moins de 10 minutes pour les TPE/PME de moins de 50 salariés, avec des primes démarrant à 800-1 500 €/an pour des capitaux de 250 000 à 1 million d'euros. **April Cyber** et **Wakam Cyber** proposent des offres similaires via des courtiers ou des plateformes en ligne. **SMABTP** et **SMACL** couvrent spécifiquement les artisans du bâtiment, les collectivités et associations, avec des offres adaptées à ces secteurs. Pour les TPE, la couverture minimale recommandée inclut la réponse à incident (accès à un CSIRT), la gestion de crise (communication), et la perte d'exploitation. Les montants assurés de 100 000 à 500 000 €, avec des franchises de 1 000 à 10 000 €, correspondent aux budgets et aux niveaux d'exposition de la plupart des TPE françaises. La sensibilisation des TPE à la cyber assurance reste un défi : selon les enquêtes, moins de 30% des PME françaises disposent d'une couverture cyber spécifique en 2025.

NIS 2 et cyber assurance : impact sur les exigences

La directive **NIS 2**, transposée en droit français fin 2024, a un impact indirect mais significatif sur le marché de la cyber assurance. D'une part, les obligations NIS 2 (gestion des risques, mesures de sécurité techniques, signalement d'incidents) créent un cadre normatif que les assureurs utilisent comme référence pour évaluer la maturité cyber des candidats à l'assurance. Une entreprise démontrant sa conformité NIS 2 présente a priori un profil de risque plus favorable. D'autre part, les nouvelles entités devenant Entités Essentielles (EE) ou Entités Importantes (EI) sous NIS 2 représentent une nouvelle cible pour les assureurs cyber, avec des besoins de couverture souvent supérieurs à leur police cyber existante (si elle existe). L'obligation de signalement d'incidents NIS 2 (24h pour notification initiale, 72h pour rapport détaillé à l'ANSSI) est parallèle aux obligations contractuelles de notification à l'assureur — les entreprises doivent coordonner ces deux flux de notification pour éviter les délais qui pourraient affecter leur couverture. Certains assureurs beginnt à proposer des certifications de conformité NIS 2 ou des audits de conformité dans leur offre de services, créant une valeur ajoutée au-delà de la pure indemnisation.

Tendances 2026-2027 : cyber assurance paramétrique et réassurance

Le marché de la cyber assurance évolue vers de nouveaux modèles en 2026-2027. La **cyber assurance paramétrique** — qui déclenche automatiquement un paiement forfaitaire dès qu'un événement paramétrique prédéfini est constaté (détection d'un ransomware confirmée par un tiers technique, indisponibilité du SI supérieure à X heures) — élimine les délais d'expertise et les litiges sur les montants de pertes. Plusieurs assureurs expérimentent ce modèle en Europe. Le renforcement de la **réassurance cyber** par des pools dédiés (Pool RE Cyber en France, similaire au Pool Re britannique) est à l'étude pour garantir la solvabilité du marché face à un scénario de sinistre systémique (attaque cyber majeure touchant simultanément des milliers d'entreprises). L'**intégration IoT et OT** dans les polices cyber va s'accélérer avec la multiplication des équipements connectés en entreprise. Enfin, la **tarification dynamique** basée sur la posture cyber en temps réel (via des outils de monitoring continu comme BitSight ou SecurityScorecard)

devrait progressivement remplacer les questionnaires annuels statiques, créant un système où la prime reflète la sécurité réelle de l'entreprise à chaque instant.

Cyber assurance collective : pools sectoriels et mutuelles

Pour les PME et les organisations de taille intermédiaire, des solutions de **cyber assurance collective** via des pools sectoriels ou des mutuelles émergent comme une alternative intéressante aux polices individuelles. Ces dispositifs permettent de mutualiser les primes et les risques entre membres d'un même secteur, d'obtenir des conditions de souscription plus favorables grâce au volume, et de bénéficier de services de prévention mutualisés. En France, plusieurs initiatives sectorielles sont en cours. Les **groupements d'achats** organisés par des fédérations professionnelles (Fédération Française du Bâtiment, MEDEF territorial, CCI) permettent aux PME membres de souscrire une cyber assurance collective à des tarifs négociés. Des **pools de réassurance sectoriels** sont en discussion pour les secteurs les plus exposés (santé, eau, énergie) afin de garantir la disponibilité de capacité assurancielle même en cas de sinistralité élevée. Ces solutions collectives ont des limites : les couvertures sont standardisées et peuvent ne pas correspondre parfaitement aux besoins spécifiques de chaque membre, et les délais de traitement des sinistres peuvent être plus longs. Pour les entreprises ayant des besoins très spécifiques (couverture OT, internationale, montants très élevés), une police individuelle reste préférable malgré son coût supérieur.

ISO 27001 et cyber assurance : l'impact de la certification

La certification **ISO 27001** est l'un des signaux positifs les plus efficaces pour un assureur cyber. Elle démontre l'existence d'un Système de Management de la Sécurité de l'Information (SMSI) structuré, audité par un tiers indépendant, couvrant l'ensemble des domaines de sécurité. En pratique, une entreprise certifiée ISO 27001 peut obtenir des réductions de prime de 10 à 25% selon les assureurs, et bénéficie d'un questionnaire de souscription allégé — la certification

servant de présomption de maturité pour de nombreux contrôles. Les annexes A de l'ISO 27001 (114 contrôles dans la version 2013, 93 dans la version 2022) couvrent directement les exigences des assureurs : contrôles d'accès (A.9), cryptographie (A.10), sécurité physique (A.11), sécurité des opérations (A.12), sécurité des communications (A.13), gestion des incidents (A.16). Pour les entreprises en cours de certification, présenter le gap analysis et le plan de mise en conformité ISO 27001 au moment de la souscription permet déjà d'obtenir des conditions favorables, en anticipation de la certification. La certification ISO 27001 n'est pas une garantie absolue — elle documente des processus mais ne garantit pas leur application quotidienne — mais elle constitue un signal de maturité reconnu par l'ensemble du marché cyber assurantiel.

Intégration de la cyber assurance dans la gouvernance des risques

La cyber assurance ne doit pas être gérée en silo par le service juridique ou la direction financière, mais intégrée dans la **gouvernance globale des risques cyber** pilotée par le RSSI. Le premier point d'intégration est l'**analyse des risques** : les risques cybersécurité identifiés dans le registre de risques de l'entreprise doivent être classés selon leur caractère assurable ou non (les amendes RGPD ne sont pas assurables, les pertes d'exploitation lo sont). Le transfert assurantiel est une des quatre options de traitement du risque (accepter, atténuer, transférer, éviter) — il doit être choisi en connaissance de cause, pas par défaut. Le deuxième point d'intégration est le **plan de continuité d'activité (PCA)** : la police cyber doit être cohérente avec le PCA — les délais de carence de la couverture perte d'exploitation doivent être inférieurs à la durée de tolérance aux interruptions définie dans le PCA. Le troisième point d'intégration est le **budget sécurité** : la prime cyber fait partie intégrante du budget de gestion des risques cyber, à équilibrer avec les investissements préventifs. En règle générale, investir dans la prévention (réduire la probabilité et l'impact des sinistres) est plus efficace qu'augmenter les primes, mais la combinaison optimale dépend du profil de risque spécifique de l'entreprise. La formalisation de cette intégration dans un tableau de bord risque cyber présenté au comité de direction est une pratique de gouvernance de plus en plus attendue par les commissaires aux comptes et les agences de notation financière.

Comparer les polices cyber : grille d'analyse pratique

Comparer des polices de cyber assurance est un exercice complexe car les libellés varient considérablement entre assureurs, rendant les comparaisons directes difficiles. Une grille d'analyse pratique doit s'articuler autour de sept dimensions. Premièrement, la **définition du sinistre** : le déclencheur de la couverture — certaines polices déclenchent sur la "découverte" d'un incident, d'autres sur l'"occurrence" (ce qui peut créer des différends pour les incidents à révélation tardive comme les APT longue durée). Deuxièmement, les **événements couverts** : ransomware, BEC, violation de données, attaque DDoS, erreur humaine, panne système — vérifier que votre principal risque identifié est bien couvert. Troisièmement, les **montants et sous-limites** : le montant global ne dit pas tout — vérifier les sous-limites par type de couverture (extorsion, perte d'exploitation, notification, amende) car certaines sont très inférieures au plafond global. Quatrièmement, les **franchises** : montant, type (absolue ou relative), applications aux différents types de sinistres. Cinquièmement, les **prestataires de réponse à incident** : liste fermée ou libre choix ? Les prestataires listés sont-ils compétents pour votre secteur ? Sixièmement, les **territoires couverts** : votre police couvre-t-elle les incidents survenant dans vos filiales étrangères ou via vos prestataires à l'étranger ? Septièmement, les **exclusions** : la clause cyber guerre, les vulnérabilités connues non patchées, les incidents liés à une certification non maintenue — autant de clauses qui peuvent vider la couverture de sa substance dans les scénarios les plus probables.

Cyber assurance sectorielle : particularités santé, finance et industrie

Certains secteurs présentent des profils de risque cyber suffisamment spécifiques pour justifier des offres d'assurance sectorielles. Le secteur de la **santé** est particulièrement exposé : données personnelles de santé très sensibles, criticité des systèmes (vies en jeu lors d'une cyberattaque sur un hôpital), nombreux équipements médicaux connectés avec peu de contrôles de sécurité. Les assureurs spécialisés proposent des polices incluant des couvertures spécifiques (frais de notification de violation des données de santé, responsabilité civile médicale cyber). Le secteur **financier** (banques, assurances, fintech) est soumis à une réglementation renforcée (DORA

depuis janvier 2025) et à des exigences de résilience opérationnelle plus strictes — les polices cyber financières incluent typiquement des couvertures fraude financière renforcées et des délais de carence de perte d'exploitation très courts. Le secteur **industriel**, comme vu précédemment, nécessite des extensions OT spécifiques. Pour les **avocats, notaires et experts-comptables**, la responsabilité professionnelle cyber est un produit hybride couvrant à la fois les incidents de cybersécurité et les erreurs professionnelles liées aux systèmes d'information. L'assurance cyber sectorielle permet une adéquation plus fine entre le profil de risque réel et les couvertures proposées, évitant les surprimes liées à des risques inexistants dans le secteur.

Déclaration d'un sinistre cyber : pièges à éviter

La déclaration d'un sinistre cyber à l'assureur est un acte juridique dont les erreurs peuvent avoir des conséquences financières importantes. Plusieurs pièges fréquents sont à éviter. Le premier est le **retard de déclaration** : dépasser le délai contractuel de notification (24 à 72 heures selon les polices) est une cause de déchéance partielle ou totale de garantie. Ce délai court à compter de la découverte de l'incident, pas de la confirmation de son ampleur. En cas de doute sur la qualification d'incident déclarable, il vaut mieux notifier trop tôt que trop tard. Le deuxième piège est la **fausse déclaration par omission** : minimiser l'ampleur de l'incident lors de la déclaration initiale pour éviter une majoration de prime peut être requalifié en réticence et conduire à une réduction d'indemnisation. Le troisième piège est de prendre des **décisions irréversibles** (payer la rançon, effacer des systèmes compromis) avant d'avoir notifié l'assureur et obtenu son aval. Ces décisions peuvent être couvertes ou non selon les conditions particulières — sans accord préalable, l'assureur peut contester la nécessité ou le montant. Le quatrième piège est de **choisir un prestataire CSIRT non agréé** par l'assureur si la police impose une liste de prestataires approuvés — les frais d'intervention d'un CSIRT non agréé pourraient ne pas être remboursés.

Impact sur la prime après un sinistre : ce qu'il faut anticiper

Déclarer un sinistre cyber a des **conséquences sur la prime** lors du renouvellement qu'il faut anticiper pour éviter les mauvaises surprises. En règle générale, un premier sinistre entraîne une majoration de prime de 20 à 50% au renouvellement, voire un refus si le sinistre révèle des lacunes sécurité importantes non corrigées. Un deuxième sinistre dans les 3 ans suivant le premier peut conduire à un non-renouvellement. Cette dynamique crée une situation délicate pour les entreprises victimes de ransomware récidivistes — une réalité plus courante qu'on ne l'imagine, car les groupes ransomware reviennent parfois cibler une victime qui a payé la rançon, ayant démontré sa capacité et sa volonté de payer. Pour atténuer l'impact sur la prime post-sinistre, le dossier de renouvellement doit démontrer les **mesures correctives mises en place** suite à l'incident : rapport de remédiation, nouvelles mesures de sécurité déployées, formation renforcée. Un audit PASSI post-incident attestant du renforcement de la posture peut neutraliser partiellement l'impact négatif du sinistre. Changer d'assureur après un sinistre est possible mais les antécédents doivent être déclarés honnêtement — la non-déclaration d'un sinistre passé est une cause de nullité du nouveau contrat.

Gestion des sous-traitants dans la cyber assurance : la supply chain

La **sécurité de la chaîne d'approvisionnement** est devenue un critère d'évaluation à part entière dans les questionnaires de souscription cyber. Les assureurs ont pris conscience, après les incidents SolarWinds (2020) et Kaseya (2021), que la compromission d'un sous-traitant pouvait déclencher des sinistres en cascade chez des centaines d'entreprises assurées. En 2026, les questionnaires incluent systématiquement des questions sur l'évaluation sécurité des fournisseurs critiques, les contrats imposant des niveaux de sécurité minimaux, les droits d'audit des fournisseurs, et les mécanismes de détection d'anomalies dans les accès fournisseurs. Pour les entreprises ayant de nombreux sous-traitants IT (infogéreurs, hébergeurs, éditeurs de logiciels en mode SaaS), l'assureur peut imposer une cartographie des risques tiers et des attestations de conformité (certifications ISO 27001, audits SOC 2 Type II) pour les fournisseurs les plus critiques. La responsabilité civile cyber est étendue aux dommages causés à des tiers via un

fournisseur compromis — ce qui crée des couvertures croisées complexes entre la police de l'entreprise et celles de ses fournisseurs. La rédaction des clauses contractuelles de sécurité avec les fournisseurs doit être cohérente avec les conditions de la police cyber pour éviter des gaps de couverture.

Cyber assurance et télétravail : risques et couvertures spécifiques

La généralisation du **télétravail** depuis 2020 a créé de nouvelles vulnérabilités — postes personnels non maîtrisés, réseaux domestiques non sécurisés, utilisation d'outils collaboratifs non approuvés — qui ont modifié le profil de risque des entreprises. Les assureurs cyber ont adapté leurs couvertures en conséquence. Les incidents survenant sur des **équipements personnels en télétravail** sont couverts par la plupart des polices si les données professionnelles ou les systèmes de l'entreprise sont compromis, indépendamment du fait que l'incident soit survenu sur un équipement privé. Cependant, certaines polices excluent les incidents résultant de l'utilisation d'équipements personnels non conformes aux politiques de sécurité de l'entreprise — une exclusion contestable mais présente. Pour les entreprises où le télétravail est structurel (pure players du numérique, sociétés de services), les assureurs demandent des preuves que la politique de sécurité couvre les travailleurs à distance : VPN obligatoire, chiffrement du disque, politique BYOD documentée. Le déploiement du MFA est encore plus critique en contexte de télétravail car les accès distants sont le vecteur d'attaque dominant lorsque le périmètre réseau physique est supprimé.

Cybersécurité préventive financée par l'assureur : services inclus

Un avantage souvent méconnu des polices cyber premium est l'accès à des **services de prévention** inclus dans la prime. Ces services varient selon les assureurs mais incluent typiquement : un accès à une plateforme de formation anti-phishing et sensibilisation (Proofpoint, KnowBe4, ou équivalent en marque blanche) ; un scan externe de vulnérabilités

récurrent (mensuel ou trimestriel) permettant d'identifier les exposures visibles depuis Internet ; un accès à une ligne téléphonique de conseil en cas d'incident mineur (avant déclaration de sinistre) pour orienter la réponse sans engager immédiatement la franchise ; et des templates de plan de réponse aux incidents personnalisables. Beazley propose son service "Breach Response Team" (BRT) permettant d'accéder 24h/7j à des experts CSIRT avant même la déclaration d'un sinistre. AXA XL propose des audits de phishing et des formations personnalisées à ses assurés. L'utilisation de ces services préventifs est fortement recommandée — ils permettent d'améliorer la posture cyber tout en restant dans le cadre contractuel assurantiel, et leur utilisation peut influencer favorablement le renouvellement de la prime.

Sinistre en cours d'assurance : le rôle du RSSI dans la gestion de crise

En cas de sinistre cyber couvert par une assurance, le **RSSI (Responsable de la Sécurité des Systèmes d'Information)** se retrouve au cœur d'une gestion de crise multi-acteurs complexe. Sa mission est de coordonner simultanément la réponse technique (avec le CSIRT interne ou externe), la communication avec l'assureur (justifications techniques, accès aux systèmes pour l'expertise), la gestion des obligations réglementaires (notification CNIL, rapport ANSSI NIS 2), et la communication interne (direction, équipes métier). Pour être efficace dans cette coordination de crise, le RSSI doit avoir préparé en amont plusieurs éléments : un plan de réponse aux incidents documenté et testé, les contacts de l'assureur et du CSIRT mandaté disponibles hors ligne (pas seulement dans le SI compromis), une liste de contacts des parties prenantes clés (DPO, DG, juriste, équipe communication), et une compréhension claire des conditions de la police cyber (délais de notification, prestataires autorisés, conditions de la couverture extorsion). Le RSSI qui n'a jamais lu sa police cyber risque de faire des erreurs opérationnelles lors d'un sinistre qui affecteront l'indemnisation. La lecture de la police cyber et la participation aux négociations de renouvellement font partie intégrante des responsabilités du RSSI en 2026.

FAQ — Cyber Assurance 2026

La cyber assurance est-elle obligatoire pour les entreprises françaises ?

Non, la cyber assurance n'est pas légalement obligatoire en France en 2026. Cependant, elle est fortement recommandée par l'ANSSI et Cybermalveillance.gouv.fr, et de plus en plus imposée contractuellement par les donneurs d'ordres à leurs sous-traitants (notamment dans les secteurs aérospatial, défense, industrie pharmaceutique). NIS 2 n'impose pas explicitement de cyber assurance, mais les obligations de gestion des risques et de continuité d'activité qu'elle impose rendent une couverture assurantielle quasiment indispensable pour les Entités Essentielles.

Mon assureur peut-il refuser d'indemniser si je n'avais pas de MFA au moment du sinistre ?

Oui, potentiellement. Les polices cyber souscrites après 2022 incluent généralement des déclarations de l'assuré affirmant disposer de certains contrôles (dont le MFA). Si un sinistre révèle que ces contrôles n'étaient pas en place malgré la déclaration, l'assureur peut invoquer la fausse déclaration ou la réticence et réduire ou annuler l'indemnisation. C'est pourquoi la sincérité du questionnaire de souscription est indispensable. Si votre MFA n'est pas déployé à 100%, indiquez-le honnêtement — l'assureur peut accepter avec une surprime ou des conditions particulières.

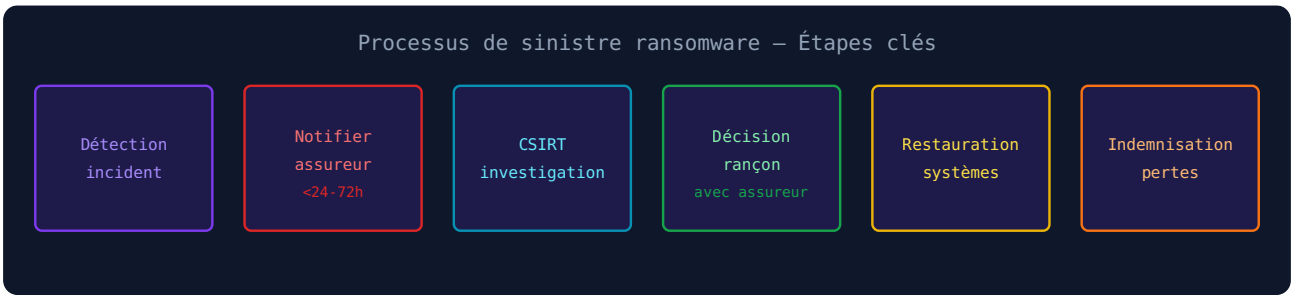
La rançon payée lors d'un ransomware est-elle remboursée par l'assureur cyber ?

Conditionnellement. La couverture extorsion/ransomware existe dans la plupart des polices complètes, mais sous plusieurs conditions : notification préalable à l'assureur avant tout paiement, validation par l'assureur ou son CSIRT mandaté que le paiement est la meilleure option, vérification que le groupe ransomware n'est pas sanctionné (liste OFAC), et preuve que les tentatives de récupération sans paiement ont été épuisées. Le montant de la rançon est généralement couvert avec un plafond défini dans la police (souvent 500 000 à 5 millions d'euros selon la taille de l'entreprise).

Comment choisir entre une franchise basse et une franchise élevée ?

Le choix de franchise doit refléter votre capacité financière d'absorption et votre profil de risque. Une franchise basse (5 000-10 000 €) protège contre les petits incidents fréquents (tentatives BEC mineures, violations de données limitées) mais génère une prime plus élevée. Une franchise élevée (50 000-200 000 €) est adaptée aux entreprises qui peuvent absorber les incidents mineurs sur leur trésorerie et cherchent à se protéger principalement contre les sinistres majeurs (ransomware paralysant, BEC de grande ampleur). La majorité des PME françaises choisissent des franchises entre 10 000 et 50 000 €, ce qui représente un bon équilibre entre protection et coût de la prime.

Assureur	Spécialité	Cible	Point fort
AXA XL Cyber	Généraliste	ETI / Grands comptes	Couverture complète, réseau mondial
Allianz Cyber	Généraliste	PME / ETI	Offre packagée, services préventifs
Hiscox	Cyber spécialiste	TPE / PME / ETI	Souscription en ligne, réactivité sinistres
Beazley	Cyber spécialiste	ETI / Grands comptes	Excellence réponse incident, BRT
Chubb Cyber ERM	Généraliste	Grands comptes	Couverture OT/ICS, internationale
SMABTP / SMACL	Mutualiste	Collectivités, BTP, associations	Tarifs adaptés secteur public



Pour une approche globale de votre stratégie cyber, consultez notre guide sur la conformité NIS 2, notre analyse du pentest OT pour les industriels, et notre comparatif des outils SOC pour optimiser votre posture. Pour les entreprises aéronautiques, notre article sur AirCyber et les exigences fournisseurs traite des liens entre conformité sectorielle et assurabilité. Côté externe, le

guide cyber assurance de Cybermalveillance.gouv.fr et les publications de la Fédération Française de l'Assurance (FFA) constituent des ressources de référence pour les entreprises françaises.

