AYI NEDJIMI Consultants

Assurance cyber 2026 : critères, exclusions et conseils

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

Décryptez le marché de l'assurance cyber en 2026. Critères de souscription, exclusions de guerre, négociation et intégration dans la gestion des.

Résumé exécutif

Le marché de l'assurance cyber a connu un durcissement significatif depuis 2021 avec une augmentation des primes, un renforcement des critères de souscription et un élargissement des exclusions contractuelles qui transforment radicalement les conditions d'accès à la couverture assurantielle pour les organisations françaises et européennes. Ce guide analyse en profondeur les critères d'éligibilité exigés par les assureurs cyber en 2026, les exclusions contractuelles les plus fréquentes à connaître impérativement avant la souscription, les stratégies de négociation pour obtenir les meilleures conditions tarifaires, et les bonnes pratiques de gestion du contrat tout au long de sa durée de vie, en fournissant aux RSSI et aux risk managers les clés pour transformer l'assurance cyber d'une dépense subie en un levier stratégique de transfert de risque intégré dans leur dispositif global de gestion des risques numériques.

L'assurance cyber est passée en quelques années d'un produit de niche proposé par une poignée d'assureurs spécialisés à un marché structuré mais tendu où la sinistralité croissante liée aux attaques par ransomware a profondément modifié l'équilibre entre les primes collectées et les indemnisations versées. Les assureurs ont réagi en durcissant considérablement leurs **critères de souscription**, exigeant désormais des preuves tangibles de maturité cybersécurité avant d'accepter de couvrir une organisation. Le questionnaire de souscription qui tenait sur deux pages en 2019 s'étend maintenant sur vingt à trente pages et couvre l'ensemble des domaines de la sécurité de l'information, du contrôle d'accès à la gestion des sauvegardes en passant par la segmentation réseau et la sensibilisation des collaborateurs. Parallèlement, les *exclusions contractuelles* se sont multipliées et précisées, créant des zones de couverture floues que seule une lecture attentive et experte des conditions particulières permet d'identifier. Pour le RSSI et le risk manager, cette évolution du marché impose une double compétence : maîtriser les exigences techniques des assureurs pour garantir l'éligibilité de l'organisation, et comprendre finement les mécanismes contractuels de l'assurance pour optimiser la couverture obtenue et éviter les mauvaises surprises lors de la déclaration d'un sinistre, en lien avec la stratégie globale de gestion des risques numériques.

Quels critères de souscription exigent les assureurs en 2026 ?

Les critères de souscription des assureurs cyber se sont standardisés autour d'un ensemble d'exigences minimales considérées comme des prérequis non négociables en 2026. L'**authentification multi-facteurs** (MFA) déployée sur l'ensemble des accès distants, des

comptes administrateurs et des accès aux applications critiques est devenue le critère numéro un : aucun assureur sérieux n'accepte de couvrir une organisation qui ne l'a pas déployé intégralement. La **gestion des sauvegardes** avec des copies immutables et déconnectées du réseau testées régulièrement est le deuxième critère éliminatoire majeur.

Les autres critères systématiquement évalués incluent la **segmentation réseau** empêchant la propagation latérale d'un attaquant, la **gestion des correctifs de sécurité** avec des délais de déploiement définis pour les vulnérabilités critiques, la **protection des endpoints** via un EDR déployé sur l'ensemble du parc, le **plan de réponse aux incidents** documenté et testé, la **sensibilisation des collaborateurs** incluant des campagnes de phishing simulé, et la *gestion des accès privilégiés* via une solution PAM. L'ensemble de ces exigences techniques doit être articulé avec votre approche de sécurité réseau Zero Trust et de gestion des vulnérabilités.

Avez-vous relu attentivement les exclusions de votre contrat d'assurance cyber, ou supposez-vous que vous êtes couvert pour tous les scénarios de sinistre sans avoir vérifié les conditions détaillées ?

Quelles exclusions surveiller dans le contrat d'assurance cyber ?

Les exclusions contractuelles constituent le piège principal de l'assurance cyber et méritent une attention particulière lors de la négociation et de la souscription. L'exclusion de **guerre et cyberguerre** (war exclusion) est la plus controversée : les assureurs ont introduit des clauses excluant les actes de guerre cyber attribués à des États ou agissant pour le compte d'États, ce qui peut potentiellement exclure les attaques de groupes APT étatiques qui représentent une part significative de la menace. La rédaction de cette clause varie considérablement d'un assureur à l'autre et nécessite une analyse juridique minutieuse.

Les autres exclusions fréquentes incluent la **non-conformité aux standards de sécurité** déclarés lors de la souscription (si l'assureur peut démontrer que les mesures de sécurité déclarées n'étaient pas effectivement en place au moment du sinistre, la couverture peut être refusée), les **actes intentionnels ou frauduleux** d'employés ou de dirigeants, les **infrastructures obsolètes** non supportées par l'éditeur (systèmes en fin de vie), les **amendes et sanctions réglementaires** dans certaines juridictions où leur assurabilité est contestée, et les **pertes de propriété intellectuelle** dont l'évaluation est souvent exclue du périmètre d'indemnisation standard. Le plan de réponse aux incidents doit intégrer les procédures de déclaration de sinistre à l'assureur.

Mon avis : L'assurance cyber n'est pas un substitut à une bonne cybersécurité mais un complément de transfert du risque résiduel. J'ai vu trop d'organisations souscrire une police d'assurance cyber en pensant avoir résolu leur problème de cybersécurité sans investir dans les mesures de protection fondamentales. Résultat prévisible : lors du sinistre, l'assureur invoque la clause de non-conformité aux déclarations de souscription et refuse l'indemnisation. L'assurance cyber doit être le dernier étage de la fusée, pas le premier.

Critère de souscription	Niveau exigé 2026	Impact sur la prime	Éliminatoire si absent
MFA sur accès distants et admins	Déploiement intégral 100%	Réduction 15-25%	Oui
Sauvegardes immutables testées	Règle 3-2-1-1, test trimestriel	Réduction 10-20%	Oui
EDR sur l'ensemble du parc	Couverture supérieure à 95%	Réduction 10-15%	Oui (depuis 2024)
Segmentation réseau	Micro-segmentation IT/OT	Réduction 5-10%	Non mais fortement recommandé
Gestion des correctifs	Critiques sous 72h, importants sous 30j	Réduction 5-10%	Non mais facteur d'évaluation
Solution PAM	Comptes admin en coffre-fort	Réduction 10-15%	Selon assureur
Plan de réponse incidents	Documenté et testé annuellement	Réduction 5-10%	Non mais fortement recommandé

L'affaire Merck contre Ace American Insurance illustre parfaitement les enjeux de l'exclusion de guerre en assurance cyber. Après l'attaque NotPetya de 2017 attribuée à la Russie, l'assureur a invoqué l'exclusion de guerre pour refuser une indemnisation de 1,4 milliard de dollars. Le tribunal du New Jersey a finalement donné raison à Merck en 2023, jugeant que l'exclusion de guerre traditionnelle ne s'appliquait pas aux cyberattaques. Cette décision a conduit les assureurs à réviser et préciser leurs clauses d'exclusion de cyberguerre, créant un paysage contractuel plus complexe que les RSSI doivent maîtriser en lien avec leur démarche de conformité réglementaire.

Comment négocier les meilleures conditions d'assurance cyber ?

La négociation d'un contrat d'assurance cyber optimal nécessite une préparation rigoureuse et une connaissance fine du marché assurantiel. La première étape consiste à préparer un **dossier de souscription exemplaire** incluant non seulement les réponses au questionnaire mais également les preuves tangibles de maturité : certification ISO 27001, rapports d'audit récents, résultats de tests d'intrusion, métriques du programme de sensibilisation et historique de sinistralité. Un dossier complet et transparent facilite le travail de l'assureur et démontre le sérieux de l'organisation.

La deuxième étape est de faire jouer la **concurrence entre les assureurs** en sollicitant au minimum trois à cinq cotations auprès d'assureurs spécialisés cyber, idéalement via un courtier expert du marché cyber qui connaît les appétences et les critères de chaque porteur de risque. La troisième étape est de négocier les exclusions et les conditions de garantie en se concentrant sur les clauses qui peuvent être amendées : périmètre de la clause de guerre, définition des événements couverts, franchise, délai de carence et plafonds par sinistre et par an.

L'accompagnement par un courtier spécialisé est fortement recommandé pour les contrats significatifs. L'ensemble s'articule avec l'hygiène informatique recommandée par l'ANSSI et les standards de l'ENISA.

Pourquoi intégrer l'assurance dans la stratégie globale de risques ?

L'assurance cyber doit être positionnée comme un outil de **transfert du risque résiduel** intégré dans la stratégie globale de gestion des risques de l'organisation, et non comme une solution isolée. La cartographie des risques cyber identifie les scénarios de risque et évalue le niveau de risque brut. Les mesures de sécurité réduisent le risque à un niveau résiduel. L'assurance cyber transfère une partie de ce risque résiduel à l'assureur, le solde étant accepté formellement par la direction.

Cette intégration stratégique implique d'aligner les garanties du contrat d'assurance sur les scénarios de risque prioritaires identifiés dans la cartographie des risques, de dimensionner les plafonds de garantie en fonction de l'exposition financière estimée pour chaque scénario, de vérifier que les exclusions ne créent pas de lacunes de couverture sur les scénarios critiques, et de mettre à jour le contrat lors de chaque évolution significative du profil de risque de l'organisation. Le RSSI et le risk manager doivent collaborer étroitement avec la direction financière et le courtier pour maintenir cette cohérence dans la durée.

Comment déclarer un sinistre cyber efficacement ?

La gestion efficace d'une déclaration de sinistre cyber conditionne directement le montant de l'indemnisation obtenue et la rapidité de la prise en charge par l'assureur. La première règle est de **notifier l'assureur dans les délais contractuels** prévus par les conditions particulières, typiquement 48 à 72 heures après la découverte de l'incident. Un retard de notification peut constituer un motif de réduction voire de refus d'indemnisation. La notification doit être précise sur la nature de l'incident, la chronologie connue et les premières mesures prises.

La deuxième règle est de **documenter minutieusement** tous les aspects du sinistre : chronologie détaillée des événements, mesures de réponse mises en œuvre, coûts engagés (factures de prestataires forensic, communication de crise, mobilisation d'équipes supplémentaires), pertes d'exploitation quantifiées et communications avec les autorités. Cette documentation constitue la base du dossier d'indemnisation. La troisième règle est de suivre les recommandations de l'assureur concernant les prestataires de réponse à incident, car la plupart des contrats prévoient des panels de prestataires agréés dont l'utilisation conditionne la prise en charge des frais.

Comment préparer le renouvellement annuel de l'assurance cyber ?

Le renouvellement annuel du contrat d'assurance cyber est une opportunité stratégique pour renégocier les conditions de couverture à la lumière de l'évolution de la maturité cybersécurité de l'organisation et des tendances du marché assurantiel. La préparation doit commencer trois à quatre mois avant la date d'échéance avec la mise à jour du dossier de souscription intégrant les améliorations apportées au dispositif de sécurité depuis la dernière souscription ou le dernier renouvellement : déploiement de nouvelles solutions techniques, obtention de certifications, résultats des derniers audits et tests d'intrusion, métriques de performance du SOC et du programme de sensibilisation.

La démonstration factuelle de la progression de la maturité cybersécurité constitue le levier principal pour obtenir des conditions tarifaires favorables lors du renouvellement. Les assureurs valorisent particulièrement les organisations qui peuvent démontrer une amélioration mesurable de leur posture de sécurité entre deux exercices, car cela réduit la probabilité et la sévérité des sinistres futurs. Le reporting des indicateurs de cybersécurité au format attendu par les assureurs, idéalement aligné sur les questionnaires de souscription standardisés du marché, facilite considérablement le processus de renouvellement et démontre le professionnalisme de l'approche de gestion des risques de l'organisation.

Sources et références : ANSSI · CERT-FR

Quel avenir pour le marché de l'assurance cyber ?

Le marché de l'assurance cyber est en pleine structuration avec des évolutions majeures attendues dans les prochaines années qui vont transformer les conditions de couverture et les modèles de tarification. La mutualisation des données de sinistralité entre les assureurs, facilitée par les régulateurs et les associations professionnelles, permettra une tarification plus fine basée sur des modèles actuariels robustes plutôt que sur des évaluations subjectives du risque. Les assureurs développent des partenariats avec des prestataires de cybersécurité pour proposer des offres intégrées combinant couverture assurantielle et services de prévention, détection et réponse aux incidents.

L'émergence de standards de reporting comme le cadre de l'EIOPA pour le secteur assurantiel et les taxonomies de risques cyber harmonisées facilitera la comparabilité des offres et la transparence du marché. Les technologies d'intelligence artificielle permettront aux assureurs de réaliser des évaluations de risques en continu plutôt que ponctuelles, ajustant les primes en temps réel en fonction de l'évolution de la posture de sécurité de l'assuré. Cette évolution vers un modèle dynamique transformera fondamentalement la relation entre assureur et assuré en créant une incitation permanente à l'amélioration de la cybersécurité.

À retenir : L'assurance cyber en 2026 exige une maturité cybersécurité démontrée comme prérequis de souscription. Le MFA, les sauvegardes immutables, l'EDR et le plan de réponse aux incidents sont devenus des critères éliminatoires. Lisez attentivement les exclusions,

particulièrement la clause de guerre cyber. Intégrez l'assurance dans votre stratégie globale de gestion des risques comme un outil de transfert du risque résiduel, pas comme un substitut aux mesures de protection.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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