CYBER RESILIENCE ACT : TRANSFORMATION DU STANDARD NUMÉRIQUE

En 2026, les assureurs français évoluent dans un milieu où la cybersécurité ne relève plus uniquement de la gestion des risques techniques, mais devient un **enjeu de souveraineté et de réputation.**
L'entrée en application progressive du Cyber Resilience Act (CRA) s'inscrit dans un contexte marqué par une intensification des cyberattaques. En 2025, les cyberattaques ont augmenté de **27 %** par rapport à 2024 selon le rapport du Ministère de l'Intérieur[1] et une montée des tensions géopolitiques, qui redéfinissent profondément les conditions de confiance dans l'économie numérique.
Les dernières publications sectorielles confirment cette évolution : **le cyber reste le risque n°1 des assureurs français en 2026**, devant les risques économiques et politiques, selon la cartographie prospective de France Assureurs publiée en début d'année[2] .

LE CYBER RESILIENCE ACT : DÉFINITION, CALENDRIER, IMPACTS ET SANCTIONS

1 Définition du Cyber Resilience Act

Le règlement sur la cyberrésilience (Cyber Resilience Act – CRA), paru au Journal Officiel de l'UE le 20 novembre 2024[3] établit des règles visant à **garantir la cybersécurité des produits comportant des éléments numériques (PEN) mis à disposition sur le marché européen** qu'il s'agisse de matériels, de logiciels ou de solutions hybrides. Il complète ainsi d'autres réglementations telles que la directive NIS2.

2 Champ d'application

Le Cyber Resilience Act concerne :

- Les fabricants de produits matériels ou logiciels intégrant une composante numérique sont concernés au même titre que les éditeurs de logiciels, y compris lorsque le logiciel est fourni indépendamment du matériel.
- Les importateurs mettant sur le marché de l'Union européenne des produits numériques provenant de pays tiers et les distributeurs (en tant qu'acteurs de la chaîne de mise sur le marché) doivent également se conformer au CRA.

[1] Le Rapport annuel sur la cybercriminalité 2026
[2] Cyberattaques : menace n°1 pour les assureurs en 2026
[3] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024

3 Calendrier de mise en application

Le Cyber Resilience Act, dont les premières obligations s'appliquent dès septembre 2026, impose un changement profond de paradigme : les produits numériques doivent désormais intégrer la cybersécurité "**by design and by default**", avec des obligations de gestion continue des vulnérabilités et de notification rapide des incidents.
Le graphique ci-après reprend les étapes d'entrée en application du CRA rappelés par l'ANSSI :

ADOPTION — 10 octobre 2024
Le CRA a été formellement adopté par le Conseil de l'Union européenne, marquant l'achèvement du processus législatif.

ENTRÉE EN VIGUEUR — 10 décembre 2024
Le CRA est entré en vigueur. A partir de cette date, les fabricants, les gouvernements et les autres parties prenantes disposent d'une période de transition pour se préparer à la conformité.

PRÉPARATION DES ÉTATS MEMBRES — 11 juin 2026
Les gouvernements et les autorités nationales doivents être prêts à appliquer le règlement, en particulier les dispositions des articles 35 à 51, qui concernent la surveillance du marché, les pouvoirs d'éxecution et les mécanisme de coopération.

OBLIGATION ANTICIPÉES POUR LES FABRICANTS — 11 septembre 2026
Les fabricants doivent commencer à signaler les vulnérabilités activement exploitées ainsi que les incidents de cybersécurité graves. Cela vise à assurer une protection précoce du marché interieur contre les menaces critiques.

APPLICABILITÉ COMPLÈTE — 11 décembre 2027
L'ensemble du CRA, y compris les exigences essentielles en matière de cybersécurité de l'annexe II et toutes les obligations des fabricants, devient pleinement applicable. A partir de cette date, seuls les produits conformes au CRA peuvent être mis sur le marché UE.

4 Les impacts : ce que le Cyber Resilience Act change

La prise en compte de la cybersécurité dès la phase de conception (**"security by design"**) et tout au long du cycle de vie du produit se traduit notamment par :

- L'identification et la **réduction des risques cyber** dès le développement,
- La mise en place de **mécanismes de mise à jour de sécurité**,
- **L'absence de vulnérabilités connues** lors de la mise sur le marché,
- La capacité à réagir efficacement avec une **obligation de notification** en cas d'incident ou de vulnérabilité découverte après commercialisation.

Conséquence directe : le risque cyber devient **plus lisible** mais aussi plus exposé publiquement, ce qui renforce mécaniquement son **impact réputationnel (**d'où l'intérêt de dresser une cartographie des produits intégrant des éléments numériques, établir un diagnostic de maturité cyber..etc)

5 Sanctions

Le CRA transforme la cybersécurité en **obligation réglementaire, assortie de sanctions conséquentes**. Ainsi, les entreprises qui ne respecteraient pas les obligations du CRA s'exposeront à des mesures de surveillance ou de contrôle et de sanction, pouvant aller jusqu'à :

- La **restriction ou l'interdiction de mise sur le marché** européen,
- Le **retrait ou le rappel des produits,**
- Des **amendes** pouvant atteindre **15 millions d'euros** ou **2,5 % du chiffre d'affaires annuel mondial.**

LE CYBER RESILIENCE ACT COMME FACTEUR AMBIVALENT : CONTRAINTE ET LEVIER DE RÉPUTATION

1 Un signal de confiance pour les acteurs conformes

Les assureurs capables de démontrer une conformité avancée en la matière pourront :

- Renforcer leur crédibilité auprès des clients et régulateurs,
- Se positionner comme des intermédiaires de confiance en matière de conformité,
- Réduire leur exposition réputationnelle en cas de crise.

2 Une meilleure gestion des crises cyber

Ainsi, les exigences du Cyber Resilience Act impliquent :

- Des processus de détection plus rapides,
- Une gouvernance renforcée,
- Une communication structurée.

> Cela limite les erreurs de gestion de crise, principal facteur aggravant du risque réputationnel.

3 Structuration d'un marché de la cyber assurance plus mature

Dans un marché où le cyber est devenu le premier risque sectoriel[4], la capacité à intégrer le Cyber Resilience Act devient une valeur ajoutée pour développer de nouveaux services:

- Meilleure sélection des risques,
- Optimisation des offres qui combineraient assurance et cybersécurité,
- Meilleure image auprès des grands clients entreprises.

[4] Pour les assureurs, les cyberattaques restent le risque le plus sévère | La Gazette France

Le Cyber Resilience Act traduit les objectifs affichés par les autorités européennes à savoir :

- Renforcer la résilience des produits numériques,
- Réduire les vulnérabilités exploitables à grande échelle,
- Garantir la transparence et la chaîne de confiance

Dans cet environnement, les assureurs ne sont plus jugés uniquement sur leur performance financière ou technique, mais sur leur capacité à :

- Se positionner comme tiers de confiance réglementaire,
- Gérer et se conformer,
- Préserver la confiance dans un monde numérique instable où l'IA peut être une arme à double tranchant (exploitée et par les cybers criminels et par les organismes pour couvrir les risques cyber).

👉 Le **Cyber Resilience Act** agit ainsi comme un révélateur puisqu'il **transforme la cybersécurité avec une meilleure modélisation du risque cyber**, dans un contexte où la confiance devient l'actif le plus critique du secteur assurantiel.

En 2026, deux trajectoires se dessinent :

- **Subir le CRA**, avec un risque accru de sanctions, d'incidents et d'atteinte à la réputation
- **S'en saisir comme levier stratégique**, pour renforcer la confiance, développer de nouvelles offres et consolider son positionnement dans l'économie numérique

Spécialisé dans la gestion des risques cyber, notre cabinet accompagne les organismes à chaque étape de leur mise en conformité et de la sécurisation de leur trajectoire numérique.

RENDEZ-VOUS PROCHAINEMENT
POUR UN NOUVEL ÉCLAIRAGE…
ET N'HÉSITEZ PAS À NOUS CONTACTER
POUR VOS BESOINS D'ACCOMPAGNEMENT

Cabinet de conseil en Organisation et Systèmes d'Information

Créer de la valeur et s'engager sur la réussite.
Ensemble.

Site internet
LinkedIn

COMETH Consulting - 5 rue Geoffroy Marie, 75009, Paris
www.cometh-consulting.com / contact@cometh-consulting.com