



ASSURANCE BENEM.MA sàrl au capital 500 000 DH
Agent Général
27, rue Amr Bnou Al Aas –Roches Noires-Casablanca
Tel/Fax : 0522409848-fax : 0522409837

ASSURANCES MULTIRISQUES INFORMATIQUE ET CYBER SECURITE

Introduction : l'assurance cyber est aujourd'hui un outil courant de transfert de risques, bien que les polices d'assurance cyber autonomes ne soient pas encore largement répandues. Cependant, les entreprises disposant de telles polices subissent moins de violations et réagissent plus rapidement aux différentes étapes de détection et de réponse aux incidents

I. L'assurance cyber est un élément utile d'un programme de gestion des risques

L'assurance cyber est un outil de transfert de risques qui s'inscrit dans un programme global de gestion des risques afin de compenser certains coûts liés aux incidents cyber, tels que définis dans la police. Elle ne remplace pas des contrôles et pratiques de sécurité robustes. En réalité, les assureurs imposent des exigences aux assurés. Une organisation est mieux positionnée pour obtenir une assurance cyber — et bénéficier des meilleures garanties et tarifs — lorsqu'elle dispose d'un programme de cybersécurité solide.

L'assurance cyber devient de plus en plus essentielle, notamment parce que les partenaires tiers exigent souvent une couverture comme condition de collaboration. Pour de nombreuses entreprises, l'auto-assurance n'est donc pas une option. Toutefois, certaines organisations choisissent de s'auto-assurer si elles disposent de réserves financières importantes ou si elles rencontrent des difficultés à obtenir une couverture (notamment dans les environnements industriels).

1. Les parties prenantes considèrent le transfert de risque comme un levier de gestion du risque cyber

Le risque cyber est un risque métier. Les deux sont étroitement liés, car les entreprises dépendent de plus en plus des services numériques. La gestion de ces risques est transversale, en particulier pour le transfert de risque via l'assurance cyber. Plusieurs fonctions sont impliquées : informatique, sécurité, juridique, ressources humaines et finances.

2. L'assurance cyber est perçue comme un outil stratégique : La plupart des entreprises sont couvertes, mais peu disposent de polices autonomes

3. Les entreprises s'appuient fortement sur le transfert de risque

Les grandes organisations ont des environnements informatiques plus complexes et détiennent davantage de données sensibles. Elles sont donc exposées à des coûts plus élevés en cas d'incident.

4. **L'assurance cyber influence le choix des prestataires :** Les assureurs imposent souvent une liste de prestataires agréés.
5. **Les entreprises assurées subissent moins d'incidents :** Cela s'explique par :
 - ✓ un meilleur niveau de maturité en cybersécurité
 - ✓ des exigences élevées imposées par les assureurs

Exemples de contrôles requis :

- ✓ gestion des comptes privilégiés
- ✓ authentification multifactorielle résistante au phishing
- ✓ segmentation réseau

6. Une meilleure détection et réponse aux incidents

Contrairement à une idée reçue, l'assurance cyber n'augmente pas le risque d'attaque. Au contraire, elle améliore la préparation grâce aux exigences imposées et aux ressources fournies par les assureurs grâce à :

- ✓ une Détection plus rapide
- ✓ une Réponse plus rapide
- ✓ Éradication plus rapide
- ✓ Meilleure capacité de confinement

En résumé, l'assurance cyber joue un rôle clé dans la gestion des risques modernes. Elle ne remplace pas la cybersécurité, mais elle incite les organisations à améliorer leur posture de sécurité tout en offrant un filet financier et opérationnel en cas d'incident.

II. quelles sont les garanties offertes par une multirisque informatique pour garantir une cybersécurité efficace?

Une assurance multirisque informatique (souvent intégrée à une multirisque professionnelle avec option cyber) offre plusieurs garanties complémentaires qui contribuent à une cybersécurité efficace ; elle ne remplace pas néanmoins les mesures techniques, elle finance et accompagne la gestion des incidents. Les principales garanties comprennent :

- ✓ **Garantie d'assistance et gestion de crise cyber** : Intervention 24h/24 d'experts en cybersécurité (forensic, IT, juridique) ; Aide immédiate pour identifier, contenir et corriger l'attaque ; Accompagnement dans la gestion de crise (communication, image, clients)
- ✓ **Garantie dommages aux systèmes et données** : Prise en charge de la restauration des données perdues ou corrompues ; Récupération ou reconstruction des systèmes informatiques ; Couverture des coûts de prestataires IT spécialisés

- ✓ **Garantie pertes d'exploitation** : Indemnisation des pertes financières dues à : arrêt d'activité, indisponibilité du système ; Compensation des frais pour maintenir l'activité (solutions temporaires)

2.1 Responsabilité civile liée aux données

Couverture des dommages causés à des tiers (clients, partenaires) : fuite de données ; violation de confidentialité ; Prise en charge des indemnisations

2.2 Frais juridiques et réglementaires

2.3 Prise en charge : honoraires d'avocats ; enquêtes administratives ; sanctions financières (selon contrats)

- 2.4 **Garantie fraude et cybercriminalité, Couverture des pertes liées à** : fraude informatique ; escroquerie (phishing, faux ordres de virement) ; Garantie communication et réputation ; Gestion de la communication de crise ; Actions pour protéger l'image de l'entreprise

- 2.5 **Garantie dommages matériels informatiques** : Réparation/remplacement : serveurs, ordinateurs, réseaux ; Couverture contre : surtension, incendie, vol, etc.

Limite importante : Une multirisque informatique n'assure pas la cybersécurité à elle seule : Elle intervient après ou pendant l'incident, pas en prévention, Elle exige souvent : sauvegardes, mises à jour, sécurité minimale

En collaboration avec des Cabinets de renommée internationale ou tout autre structure de votre choix, en matière de cybersécurité, nous sommes en mesure de vous apporter notre assistance dans l'élaboration d'un cahier des charges adapté à votre Organisation et à vos besoins.

Cordialement
Mohammed BENNANI -Gérant
GSM- 0661321844

Intermédiaire d'assurance régi par la loi n°17-49 portant code des assurances. Décision n°
A17625721201178082 du 6 juin 2011 E-mail : assurben35@gmail.com RC Casa n°230263 T.P N° 37949485
ICE 001443487000063