Beazley Logo

Vidéo

Episode 12 | Dans le fauteuil...Cyber | Loria Mebarki

La transformation numérique a profondément changé le fonctionnement des entreprises. Aujourd'hui, sans systèmes informatiques, plus rien ne fonctionne : production, ventes, comptabilité, relation client ou encore gestion des opérations. Dans ce contexte, le risque cyber est devenu un risque stratégique.

Une cyberattaque peut paralyser l'activité en quelques heures, compromettre des données sensibles, perturber les opérations et affecter durablement la réputation d'une entreprise. Les conséquences financières peuvent être considérables, mais l'enjeu dépasse désormais la simple indemnisation. L'assurance cyber est devenue un véritable outil de continuité d'activité.

Au-delà de la couverture financière, elle permet d'accéder rapidement à des experts capables d'accompagner les entreprises dans les moments les plus critiques. Réponse à incident, gestion de crise, communication, expertise technique ou juridique : la capacité à réagir rapidement est souvent déterminante pour limiter l'impact d'une attaque et accélérer le retour à la normale.

L'évolution du cadre réglementaire renforce également l'importance de la résilience cyber. Le règlement européen DORA impose aux acteurs du secteur financier de renforcer leur capacité à prévenir, détecter et gérer les incidents numériques, tout en surveillant davantage leurs prestataires critiques. L'objectif est clair : garantir la continuité des services financiers même en cas de crise cyber.

En France, la loi LOPMI introduit une nouvelle exigence pour les entreprises victimes d'une cyberattaque : le dépôt d'une plainte dans un délai de 72 heures pour pouvoir bénéficier de certaines garanties d'assurance. Cette mesure vise à renforcer la réactivité et la transparence dans la gestion des incidents.

Face à ces enjeux, la prévention reste la première ligne de défense. Certaines mesures simples permettent de réduire significativement l'exposition au risque : activer l'authentification multifactorielle, former

les collaborateurs aux tentatives de phishing, segmenter les accès aux systèmes sensibles et mettre en place des sauvegardes régulières.

Mais au-delà des bonnes pratiques, chaque entreprise possède un profil de risque unique. Identifier ses vulnérabilités, comprendre ses dépendances numériques et adapter ses dispositifs de protection constituent les fondements d’une stratégie cyber efficace.

Dans un environnement où les cyberattaques sont devenues une certitude plutôt qu’une éventualité, l’assurance cyber n’est plus seulement une protection. Elle est un levier essentiel de résilience, de continuité d’activité et de confiance.

Home

©Beazley Group | LLOYD's Underwriters