Beazley Logo

Le conseil d'administration est le premier responsable : Responsabilité en matière de cyber-risques

Rory Burling

La mauvaise gestion d'un incident cybernétique est un risque croissant dans le secteur de l'assurance responsabilité civile. Qu'il s'agisse d'une violation de données ou d'une cyberattaque mal gérée, les dirigeants sont de plus en plus exposés à des litiges concernant des incidents liés à la cybersécurité. en glissement annuel des cyberattaques dans le monde. Compte tenu de cette tendance, une augmentation des litiges liés aux cyberrisques est inévitable. Pour contrer cette menace, les entreprises ont besoin de :

Les entreprises ont besoin de se protéger contre la cybercriminalité.

- Investir dans les nouvelles technologies de cyberdéfense et la cybersécurité
- Des plans de continuité de l'activité répétés régulièrement qui incluent la gestion des crises et de la réputation
- Une bonne compréhension des fournisseurs tiers et de la dépendance et de la connectivité des entreprises à leur égard
- Un programme d'assurance cybernétique adapté avec une expertise en matière de gestion des sinistres.

L'évaluation du risque cybernétique dans un paysage mondial chaotique

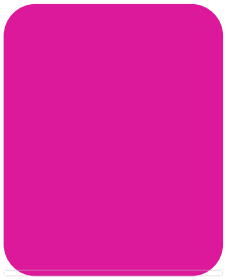
Les dirigeants sont de plus en plus confrontés à des risques cybernétiques. **23%** ne se sentaient pas préparés à contrer les menaces posées par les cyber-risques. En revanche, il est encourageant de constater que **24%** envisagent d'investir dans des mesures de défense en matière de cybersécurité afin de renforcer leur

résilience face à ce risque. **26%** ont classé le risque cybernétique en tête de leurs préoccupations cette année. Il s'agit d'un chiffre considérable qui est susceptible d'augmenter compte tenu du nombre croissant d'attaques et de la surveillance de plus en plus étroite exercée par les autorités de réglementation dans ce domaine.

Une approche à spectre complet

Une approche globale de la cybersécurité met en œuvre des mesures préventives et préventives, telles que l'analyse de l'horizon des risques afin d'identifier les angles morts et les nouvelles menaces. Si une cyberattaque conduit les investisseurs à remettre en question les compétences du conseil d'administration, les dirigeants peuvent se défendre en apportant des preuves tangibles que des mesures raisonnables ont été prises pour empêcher l'attaque, et prouver qu'ils avaient mis en place des plans de gestion active des risques et un soutien pour aider à atténuer l'impact de l'attaque.

L'entreprise et ses dirigeants devront faire face à leurs actionnaires, à leurs investisseurs et à leurs clients.



Rory Burling

Souscripteur, Solutions spécialisées, Responsabilité des dirigeants, échelle mondiale

Home

©Beazley Group | LLOYD's Underwriters