The Cyber Insurance Buyer's Checklist

5 steps to coverage that responds

01

Map your risk exposure

- What is our estimated revenue loss per day of full IT outage?
- Which processes and revenue streams depend on digital systems being available?
- Do we process personal data relating to customers, patients or employees, and in what volumes?
- Which third-party services, if disrupted, would directly affect our operations?

Your insurance broker or risk advisor can help you with this assessment.
Eye Underwriting partners with brokers across Europe and can make an introduction

02

Assess your current security posture

Insurers assess risk based on the controls in place at the time of application and throughout the policy period. Understand the baseline before application.

- Are at least 85% of our endpoints actively monitored by our security solution?
- Is multi-factor authentication (MFA enforced for remote access, email and cloud services?
- Do we have daily, immutable, encry ted backups, and have they been tested within the last 12 months?
- Do we have a documented and tested disaster recovery and business cont nuity plan?
- Are there systems accessible from the internet that are no longer actively supported by the vendor (end-of-life)?
- How much sensitive personal data do we process, how do we protect it, and are we GDPR-compliant?

03

Understand what the policy covers

The sum insured figure on the front page of a cyber policy rarely reflects the actual coverage available. Sublimits are internal caps that apply to specific types of loss, meaning individual components such as extortion, regulatory defence or business interruption may be capped well below the headline amount

- What sublimits apply, and to which coverage sections?
- Is this policy primary coverage, or does it sit in excess of other policies?
- Does coverage include third-party liability for privacy violations under the GDPR?
- Are directors and officers explicitly included as covered persons in a cyber context?
- Is incident response coverage pre authorised, or does each action require insurer approval?

04

Evaluate the incident response arrangement

How quickly and competently an insurer responds in the first hours of an incident is as commercially significant as the financial coverage provided.

- Who do we call in the first hour of a suspected incident, and what happens next?
- Does the insurer have a dedicated 24/7 incident response capability, or is it outsourced? And if outsourced, do we know who will help us and do they know our organisation?
- What actions can be taken without advance insurer approval?
- Does the deductible apply to first-response activities, or only to subsequent losses?
- How will we be kept informed during an active incident?

Note: Under Eye Seamless Cyber Cover, the deductible does not apply to Eye Security incident response activities

05

Confirm renewal and continuity terms

Insurers adjust acceptance criteria and pricing based on industry-wide loss experience, not your individual security record. A policy that is straightforward to obtain today may face a different renewal environment in 12 months. Re-evaluation is not a sign of inadequate coverage; it is a standard governance step. On what basis will renewal terms be determined: market-wide loss ratios or our individual security record?

- What security controls will be required at renewal, and how is compliance assessed?
- Will a security incident during the policy period affect renewal eligibility?
- Is there a mechanism to document and evidence our security posture continuously, rather than at a single renewal date?
- If we already hold cyber coverage: when were the sublimits and exclusions last reviewed against our current revenue and data footprint?
- Has our industry sector experienced significant cyber losses in the past 12 months that could affect our renewal terms?

A broker with dedicated cyber expertise can help you review your renewal position well in advance

Expieriencing a cyber incident?

Call the Eye Security Incident Response hotline at

+31 88 644 4898

(24/7 availability)

or contact the IR team via email at **cert@eye.security** for non-urgent cases.

About Eye Underwriting B.V.

Eye Underwriting is a specialist cyber insurance provider and part of the Eye Security ecosystem. Together, Eye Security and Eye Underwriting bring an integrated cyber resilience model to key European markets, combining MDR, incident response, and cyber insurance into one coordinated approach to risk reduction. Built for mid-sized organisations that are often underserved by traditional cyber insurance, the model provides both operational resilience and financial protection, with stable terms in an increasingly volatile market.

www.eyeunderwriting.eu

© 2026 Eye Underwriting. All rights reserved. This document is provided for information purposes only and does not contain the full terms, conditions, limitations or exclusions of the policy. Coverage is subject to the full policy wording W.02.03-NL-NL-2026 and to underwriting approval. Eye Seamless Cyber Cover is underwritten through Lloyd's Brussels. Eye Underwriting B.V. is registered with the AFM (Dutch Authority for the Financial Markets). This document does not constitute advice. Organisations should seek independent advice from a licensed insurance broker. Note on GDPR/DSGVO fines: the insurability of administrative fines depends on applicable law and jurisdiction. Coverage applies only where permitted.