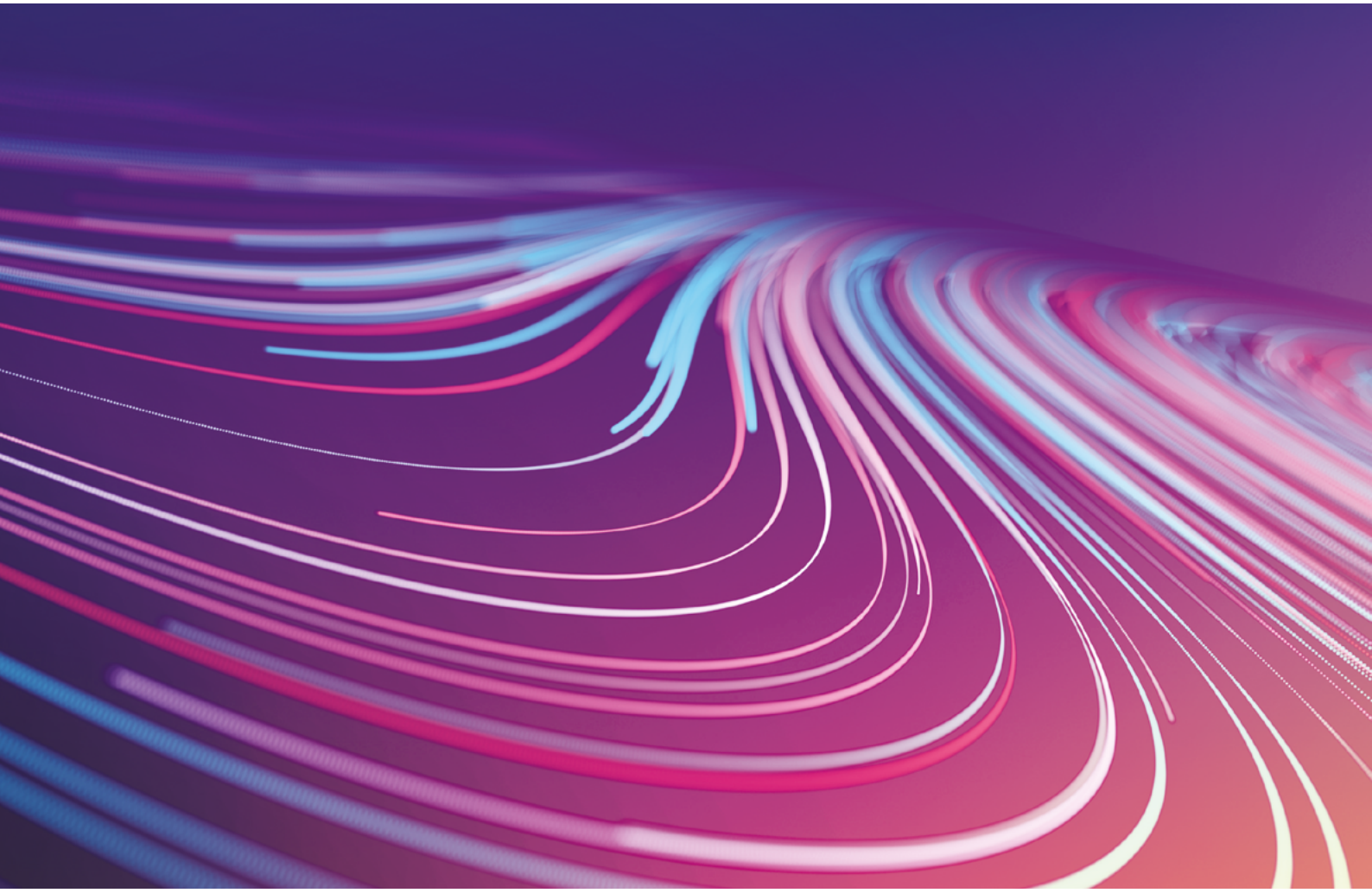
Security.
Response.
Insurance.
One system.

Cyber Insurance for a New Era of Risk

Integrating security, incident response and insurance into one system of protection



www.eyeunderwriting.eu | info@eyeunderwriting.eu

Contents

03 Foreword
04 Executive Summary
24 Contact

01 Risk

06 Cyber Risk as a Board-Level Responsibility

02 Solution

09 The Eye Seamless Model Explained
12 Security, Incident Response, and Insurance as One
13 What Happens in an Incident
14 Cyber Insurance Coverage: Scope and Triggers
15 Key Governance Considerations

03 Action

17 Getting Cyber Insurance Right
22 Why Conventional Cyber Insurance Falls Short
23 The Application Process: What to Expect

Foreword:
The Future of Cyber Resilience

The future of cyber resilience is integration.

Cyber risk is best managed when IT security, incident response, and insurance work seamlessly together.

Cyber insurance was designed for a world where security and insurance operated separately. You purchased protection, you purchased coverage, and you hoped the two would align when an incident occurred. This model is no longer fit for purpose.

Cyber attacks are faster, ever-changing, more targeted, and more damaging than ever. A single incident can halt production, destroy data, trigger regulatory action and cause reputational harm that lasts long after systems are restored. The financial impact is consistently underestimated, often by a factor of ten.

Yet the conventional response remains unchanged: a standalone policy, an external incident response provider unfamiliar with your organisation, and security controls assessed once at application. This approach leaves a critical gap in the first hours of an active incident.

The future of cyber resilience is integration. When security, incident response, and financial protection operate as a single system, detection accelerates, response is immediate, and financial impact is contained. The outcome is fundamentally different from traditional standalone insurance.

This document explains what this means for your risk exposure, your governance responsibilities, and the decisions you need to make.

Dr. Kennet K. Otto

Managing Director / Chief Underwriting Officer

Maarten de Jonge

Head of Insurance Development, Eye Underwriting

Executive Summary

Cyber incidents do not unfold as separate security, response, and insurance events. They unfold as one crisis. Yet most organisations still manage cyber risk through separate providers, separate contracts, and separate processes.

First, this creates a critical gap when speed matters most. In the first hours of an incident, security teams need to contain the threat, leadership needs clarity, insurers need notification, and external advisors may require approval before costs are incurred. Every delay increases operational disruption, financial exposure, and regulatory pressure.

Second, traditional standalone cyber insurance is based on the inventory of security controls, typically by assessing more than 100 individual controls. However, the cyber landscape evolves so rapidly that inventories which were still relevant last year may already have lost their value today.

Eye Seamless Cyber Cover is designed to close these gaps. It brings together 24/7 security monitoring, immediate incident response, and cyber insurance into one integrated system of protection. The result is a fundamentally different operating model. Detection, containment, forensic investigation, insurer coordination, and coverage alignment are connected before an incident occurs. Customers do not need to manage fragmented communication between security providers, insurers, legal advisors, and response teams during an active crisis.

For executives, the model strengthens governance. It supports board-level cyber risk management, creates clearer accountability, reduces uncertainty around incident response, and provides a more stable basis for renewal. For IT and security teams, it translates insurance obligations into practical, continuously monitored controls rather than one-off annual declarations.

Cyber resilience is no longer only about buying stronger security tools or broader insurance coverage. It is about ensuring that prevention, response, and financial protection work together when the organisation is under pressure.

Eye Seamless Cyber Cover turns cybersecurity, incident response, and insurance into one system built for the speed, complexity, and financial reality of modern cyber risk.

74%

of SMEs may be underinsured, according to Hiscox's Global Protection Gap Report 2025.

7-15%

Only 7 to 15% of European companies have cyber insurance, even though much of their value is tied to intangible assets.

€20,000+

minimum annual cost for a separate incident response retainer, which many providers charge in addition to MDR.

> *Buyers who treat MDR and cyber insurance as separate procurement decisions leave both value and coverage on the table. The most resilient mid-market programmes bring them together."*
>
> **Forrester, The State of Cyber Insurance in Europe, 2025**

01

Risk

Cyber Risk as a Board-Level Responsibility

Cyber risk is no longer an IT issue that can be delegated or ignored. It is a management responsibility. Under NIS2, management bodies of essential and important entities are required to approve cybersecurity risk-management measures, oversee their implementation, and ensure they have the knowledge needed to understand and manage cyber risk.

Across Europe, these obligations are being implemented through national laws, such as Germany's BSIG and the Dutch Cyberbeveiligingswet. The details differ by jurisdiction, but the direction is clear: boards and managing directors are expected to take an active role in cyber resilience.

Beyond regulatory penalties, general company law may also create liability exposure where management fails to exercise appropriate care and a cyber incident causes significant loss.

Failure to meet these obligations, whether intentional or negligent, can constitute a breach of duty. In the event of a cyber incident causing significant loss, this may result in personal liability for managing directors. In particular, salaried executives should expect that shareholders or supervisory boards may seek recourse to recover damages.

Cyber risks are business risks and require active management.

Financial exposure

Losses are consistently underestimated, often by a factor of 10. Business interruption, ransom demands, forensic investigation, legal costs and reputational loss compound rapidly.

Regulatory exposure

GDPR Art. 33 requires breach notification within 72 hours. The German BSI Act and NIS2 impose further obligations on critical sectors. Failures in security or breach notification may lead to fines and regulatory proceedings.

Personal liability

New EU legislation is increasing personal liability for directors and officers in the event of a cyber incident.

Closing the gaps in cyber insurance coverage

Cyber insurance only works when the details do: sublimits, exclusions, and approval processes matter.

A well-designed cyber policy covers financial losses from business interruption, ransom demands, forensic investigation and recovery. It also provides legal defence and, where permitted, covers fines arising from regulatory proceedings under GDPR and the German BSI Act. By explicitly including directors, officers and supervisory board members as insured persons, it closes the personal liability gap left by standard D&O policies.

This protection depends on how the policy is structured. Hidden sublimits, broad exclusions or approval requirements that delay response can leave critical exposures uncovered when a claim arises. Eye Seamless Cyber Cover is designed to eliminate these gaps.

02

Solution

The Eye Seamless Model Explained

Eye Seamless Cyber Cover is not a standalone policy. It is the insurance component of an integrated solution built on three interdependent elements: security, incident response and financial protection.

Together, these elements operate as a single continuous system. Eye Cyber Guard delivers 24/7 monitoring and detection. Incident response is activated immediately when a threat is identified. Eye Seamless Cyber Cover provides the financial and legal protection required to maintain continuity during an incident.

Each element reinforces the others. Stronger security reduces risk, integrated response limits impact, and continuous visibility into security performance supports more stable renewal terms. The result is a closed-loop model that continuously improves resilience and optimises risk investment.

Improved resilience and optimised risk investments

An integrated system connects prevention, response, and financial protection.

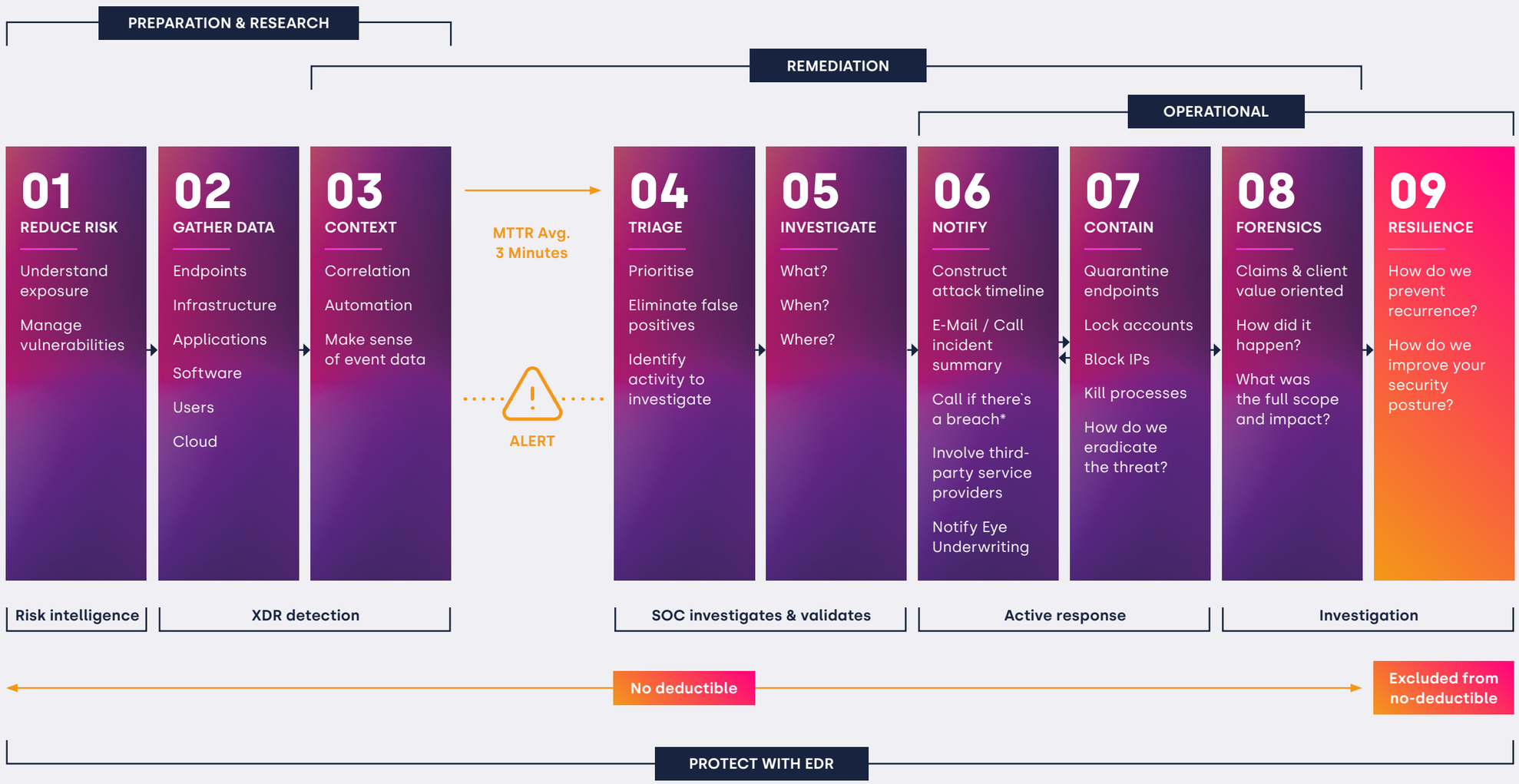
How incident response operates

This diagram shows the nine-stage process of the Eye Security incident response service, from risk reduction and detection to forensic investigation and long-term resilience.

Two points are particularly relevant:

- **No deductible from step 1 through 8**
  All activities from risk intelligence and XDR detection through triage, investigation, notification, containment and forensic analysis are covered without application of the policy deductible. This covers the full active incident lifecycle, from the first alert to the final forensic report.
- **One single point of contact**
  At step 6 (Notify), if a breach is confirmed, Eye Security contacts third-party service providers and notifies Eye Underwriting automatically. You do not need to manage parallel insurer communication in the middle of an active incident. This is a structural feature of the integrated model.

Incident response activities of Eye Security



Activities of the Eye Security incident response team: stages 1 through 8 operate under the no-deductible arrangement; stage 9 (Resilience) marks the transition to recovery and posture improvement.

The Eye Security incident response team brings deep expertise and a proven track record. Each year, the same experienced team works on more than 100 incidents at organisations of all sizes and sectors, including companies that are not yet protected by Eye Security on a day-to-day basis.

Security, Incident Response, and Insurance as One

Integrating these three elements creates clear operational and contractual advantages over standalone solutions.

Eye Cyber Guard

Continuous 24/7 monitoring of endpoints and cloud environments. The 24/7 SOC detects threats and initiates containment. Eye Security proactively informs you of insurance-relevant critical vulnerabilities, an obligation that would otherwise fall entirely on you under standard policy conditions.

Eye Incident Response

In virtually all incidents, Eye Security detects and contacts you before your internal teams are aware. A team available 24/7 handles triage, containment, forensic investigation and, where required, coordination of legal and PR advisors. No insurer pre-approval is required for any first-response activities.

Eye Seamless Cyber Cover

Primary coverage, not excess over other policies. One clear sum insured without hidden sublimits. Premiums reflect the demonstrably lower risk profile of organisations under active Eye Security monitoring. Renewal is based on documented security performance, not annual re-underwriting.

An important note on data protection

Eye Security does not share any information about your security posture, vulnerability status or incidents with Eye Underwriting or the insurer without your explicit permission. This monitoring relationship is designed entirely in your interest and is a contractual commitment.

What Happens in an Incident

The value of integration becomes most apparent during an incident. The sequence below shows how an incident unfolds under Eye Seamless Cyber Cover and how this differs from conventional insurance.

Detection

Eye Security's SOC identifies the incident. The incident response team is immediately available. In most cases, Eye proactively contacts you before your internal teams are aware. If you detect the incident first, the 24/7 Incident Hotline is available immediately: Germany +49 (0)203 6688 1900 / Netherlands +31 (0)88 644 4898.

Response

Intake, triage, stabilisation and containment begin immediately and continue. No insurer pre-approval is required. The deductible does not apply to Eye Security incident response work, forensic investigation, evidence collection and first-responder activities. There is no administrative delay.

Escalation

Where required, Eye Security coordinates specialist advisors: legal counsel, PR/communications advisors and forensic accountants. Emergency costs incurred with Eye Security's guidance do not require advance insurer approval.

Recovery

Eye Security notifies Eye Underwriting. Eye Underwriting aligns with the insurer on coverage for subsequent activities, providing clarity before additional costs are incurred. Where required, the insurer issues a formal claims approval, providing confirmation of coverage and certainty on the indemnification of costs and losses.

Cyber Insurance Coverage: Scope and Triggers

These three sections represent the coverages that matter most in a cyber incident. They are structured around the financial consequences organisations face most frequently: the immediate cost of responding to an incident, the revenue and operational losses that follow, and potential third-party claims. Full terms are set out in the policy conditions.

Section A: Incident response	**Section B:** First-party loss	**Section C:** Third-party liability
Incident response costs: triage, containment, forensic investigation, evidence collection from a team that is immediately available. No deductible applies to Eye Security first-response activities. Legal and PR advisory costs included. Cyber extortion and ransomware (insurer pre-approval required for payment). Network interruption caused by failure at a third-party service provider (supply chain). Incident types like data breaches, network security breaches, operational errors, system failure, denial-of-service attacks, extortion, cryptojacking and artificial intelligence events.	Revenue loss during the recovery period (own systems). Revenue loss during the recovery period of third party systems your depending on for essential processes. Recovery costs: data restoration, system restoration. Hardware and software replacement costs (including functional improvement where unavoidable). Reputational revenue loss: up to 180 days following negative media coverage of a covered incident.	Third-party claims arising from data breach or network security failure Privacy regulatory defence and penalties Defence costs for regulatory proceedings (including BSI / Datenschutzbehörde). PCI fines and assessments (payment card incidents). Media liability: multimedia wrongful acts via electronic media. Coverage extends to current and former directors, officers, supervisory board members and employees in their capacity as part of the covered organisation. Note: This coverage is specific to cyber events and does not replace D&O insurance.

Key Governance Considerations

Renewal stability

Because Eye Security continuously monitors and updates your security posture, it remains aligned with renewal requirements throughout the policy period. This enables ongoing engagement with insurers and materially reduces renewal risk.

CVE and patch obligations

Standard cyber policies place the obligation to monitor and remediate newly published vulnerabilities entirely on you. Under Eye Seamless Cyber Cover, Eye Security actively informs you of insurance-relevant critical vulnerabilities. This reduces the risk of inadvertent coverage gaps due to missed patches.

Aligned with your IT strategy

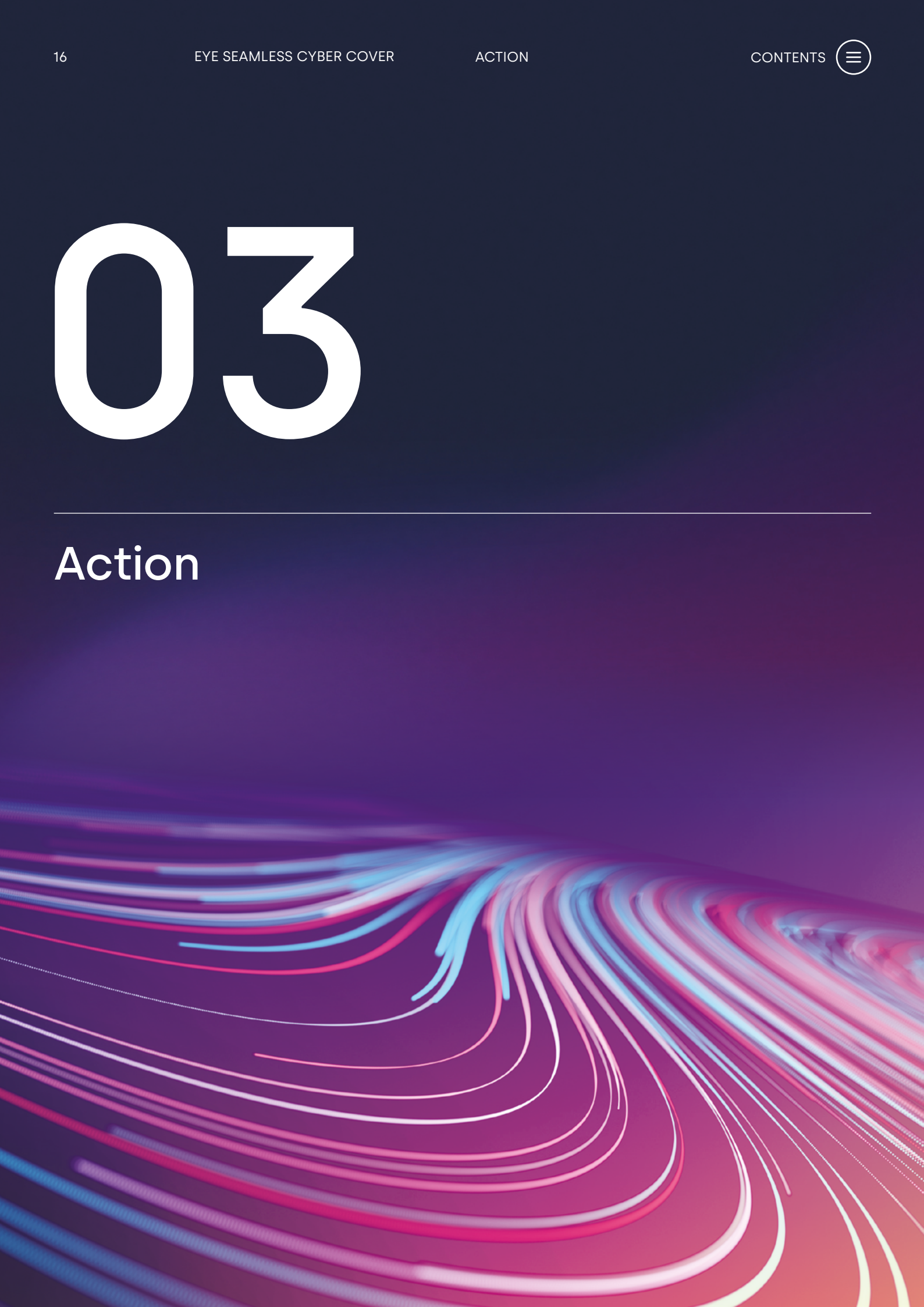
Eye Seamless Cyber Cover is designed to work with your existing IT and security roadmap. The security obligations under this policy are limited to a focused set of practical controls. Your IT team will not be burdened with requirements that conflict with your existing security strategy or architecture. Where Eye Cyber Guard is in place, most of these obligations are met as a direct result of the monitoring relationship.

Changes in 2026 policy conditions

The cyber landscape is ever-changing. Several new coverages are introduced, including new coverages for cryptojacking and AI-related system failure.

03

Action



Getting Cyber Insurance Right

Obtaining cyber insurance is a governance decision. Your involvement in understanding your organisation's risk profile, asking the right questions, and ensuring the policy structure matches your actual exposure directly determines whether the coverage you purchase will respond when it is needed.

Steps 1 to 5: Your preparation and acquisition process

01

Map your risk exposure

You should have a clear understanding of revenue exposure from a system outage, the volume and sensitivity of personal data held, dependencies on third-party IT services, and the operational consequence of a multi-day IT disruption.

- 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. Note: for German organisations, the BSI classification of your sector under the KRITIS framework may affect both your regulatory obligations and the insurance conditions available to you.

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, not to achieve a perfect score, but to ensure the application accurately reflects reality and to identify gaps that could affect coverage. For Eye Seamless Cyber Cover, the most important controls are:

- 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, encrypted backups, and have they been tested within the last 12 months?
- Do we have a documented and tested disaster recovery and business continuity 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?

As an Eye Security customer, you can find the status of most of these controls in your Eye Portal. Note: under most cyber policies, failure to maintain these controls during the policy period, not just at inception, can affect coverage. This is a continuing obligation, not a one-time declaration.

03

Understand what the policy actually 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. You should require a clear breakdown before committing.

- 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. A policy that requires advance approval before forensic investigators or legal counsel can be engaged introduces delay at the worst possible moment. You should understand the exact mechanics before an incident occurs.

- 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. In most incidents, Eye Security will initiate contact proactively.

05

Confirm renewal and continuity terms

The cyber insurance market is more volatile than most other lines. 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. This applies whether you are taking out a new policy or already hold coverage: if you have not reviewed your cyber insurance in the past year, the terms, sublimits and acceptance conditions in your current policy may no longer reflect the current threat landscape or your actual exposure. The cyber market has tightened materially since 2022, and many organisations with long-standing policies have found significant gaps at renewal that were not visible when the policy was first placed. 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, avoiding surprises at the last moment. Eye Underwriting works with a network of specialist brokers and can make an introduction. Under Eye Seamless Cyber Cover, renewal is based on your documented, continuously monitored security posture.

Aligning your risks with the right coverage

The table below maps common risk concerns to the questions they raise for insurance coverage, the policy structure required to address them, and how Eye Seamless Cyber Cover responds to each.

Risk concern	Key question	Coverage needed	Eye response
Business interruption	*How long can we survive without IT, and what does it cost per day?*	First-party BI coverage with adequate recovery period (minimum 180 days) and no sublimit below actual exposure.	BI coverage with 180-day recovery period; supply chain and system failure extensions available.
Ransomware and extortion	*Could we be locked out of our systems, and do we have a response plan?*	Cyber extortion coverage including ransom payment (subject to sanctions compliance), negotiation expertise, cryptocurrency payment and associated incident response costs.	Extortion coverage including cryptocurrency payments; insurer pre-approval required for payment; incident response team supports negotiation.
GDPR regulatory exposure	*Are we GDPR-compliant and prepared to notify the Datenschutzbehörde within 72 hours?*	Regulatory defence and fines coverage (where insurable under applicable law); breach notification support.	Regulatory defence covered; GDPR Art. 33 alignment built in; fines covered where permitted under German law.
Personal director liability	*Are we personally exposed if the company suffers a cyber incident?*	Explicit inclusion of directors, officers and supervisory board members as covered persons.	Directors, officers, supervisory board members and employees covered in cyber event context. Does not replace D&O.
Third-party and supply chain failure	*What if a key IT supplier goes down; are we covered for our losses?*	Contingent BI coverage for losses caused by failure at third-party service providers.	Contingent BI extension covers revenue loss and recovery costs from third-party provider outages.
Reputational damage	*If we appear in the press following a breach, can we recover the revenue impact?*	Reputation harm coverage with adequate duration following negative media coverage.	Reputational revenue loss covered for up to 180 days following a covered incident.
Data breach liability	*If customer or employee data is exposed, what are we liable for to third parties?*	Third-party privacy and network security liability; GDPR-aligned; including emotional and psychological harm claims.	Privacy and network security liability including GDPR/DSGVO violations and emotional harm from data exposure.
Security posture uncertainty	*Will our coverage hold if we miss a patch or have a gap in controls?*	Active vulnerability monitoring and proactive notification, not a passive ongoing obligation on you.	Eye Security actively monitors and notifies; no silent coverage gap from missed CVEs. Eye does not report posture to insurer.
Additional entities and foreign locations	*Are our subsidiaries and foreign offices covered under the same policy?*	Coverage that explicitly extends to named subsidiaries and locations, with clear rules on which geographies are included or excluded.	Locations protected by Eye Cyber Guard can be co-insured in most cases. Locations in countries on applicable sanctions or no-go lists are excluded.

A note on D&O and cyber coverage

Directors and officers liability insurance (D&O) and cyber insurance address different exposures and should not be confused. D&O covers claims arising from management decisions and breaches of duty in a broad corporate governance context. Eye Seamless Cyber Cover includes you as director or officer specifically in the context of a covered cyber event, for example a regulatory action or third-party claim that arises directly from a breach. The two policies are complementary, not interchangeable. You should review both policies jointly with your broker to ensure there are no gaps or unintended overlaps.

Why Conventional Cyber Insurance Falls Short

If you are evaluating Eye Seamless Cyber Cover in the context of an existing policy or a market comparison, the following structural limitations of conventional standalone cyber insurance are relevant.

- Application processes average around 100 questions, require extensive IT inventories, and take months to complete.
- Sublimits and exclusions, often only discovered at the point of claim, mean the actual scope of coverage is narrower than the sum insured suggests.
- Policy renewal has become increasingly difficult. Insurers revise their acceptance criteria annually based on market-wide loss experience, not individual risk quality. What was adequate coverage last year may trigger a higher deductible or non-renewal today.
- You are expected to independently monitor newly published CVEs and apply remediation within defined timeframes. Failure to do so can reduce or void coverage, an obligation that is frequently underestimated.
- Incident response typically requires advance insurer approval before costs are incurred, introducing delays at the moment speed is most critical.
- Insurers may adjust terms or coverage scope based on portfolio-level loss experience unrelated to your security posture.

Each of these limitations is structurally addressed by the Eye Seamless Model. The no-deductible incident response arrangement, active vulnerability monitoring, the documented security posture as a renewal basis, and the primary coverage structure are direct responses to known failure points in the conventional market.

The Application Process: What to Expect

The application is designed to reduce the burden on you while maintaining underwriting discipline. A premium indication is provided even where not all conditions are yet met.

01

Security implementation

Eye Seamless Cyber Cover is only available in conjunction with Eye Security's Eye Cyber Guard. Eye Cyber Guard should be operational within 30 days of policy inception.

02

Application

Complete the online questionnaire. It takes approximately 8 to 12 minutes. Even if you do not comply with all conditions immediately, you will receive full insurance information, a premium indication and guidance on how to comply.

03

Quotation

A quotation is returned within days. Coverage is available for organisations across most industries, including sectors such as manufacturing, logistics and healthcare that are typically difficult to place.

Ready to apply?

Applying for Eye Seamless Cyber Cover takes 8 to 12 minutes online. You can apply directly or through your broker. A first premium indication is provided immediately, even if not all conditions are yet met.

For full information, including coverage details, eligibility and the application form:
www.eye.security/solutions/cyber-insurance

Or contact Eye Underwriting directly at:
info@eyeunderwriting.eu

Contact

Mariam Fakiri

Underwriter, Eye Underwriting Germany and Belgium

info@eyeunderwriting.eu

René Schwering

Underwriter, Eye Underwriting The Netherlands and Belgium

info@eyeunderwriting.eu

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.