# Cyber insurance: would your policy pay after an attack?

Before your next renewal, check every questionnaire answer against your systems and keep the evidence, because a wrong answer can cost you the cover. Then read the wording on war, provider outages, ransom, payment fraud and fines, and set the limits and the indemnity period from your measured recovery time.

| Reviewed | Next review | Version |
|---|---|---|
| **5 Nov 2026** | **5 Dec 2026** | **1.0** |

Written for
**IT, security, finance and risk leads in EU organizations buying, renewing or claiming on cyber insurance, especially in Germany**

Latest version
**sheets.einblick.dev/cyber-insurance/**

## If you only do five things

1. **Answer the questionnaire from evidence, not memory.** Check each answer against your systems before you sign. Under German law, an insurer can withdraw over an intentional or grossly negligent wrong answer; it then pays only if the fact played no part in the claim, and after fraud not at all[1].
2. **Keep the policy's security duties all year.** The GDV model terms turn controls into duties, from separate admin accounts and timely patches to weekly backups and restore tests. Intentional breaches void the payout and grossly negligent ones cut it, unless you show the breach played no part[2].
3. **Call the insurer before you hire anyone.** The GDV model pays forensics only after prior coordination with the insurer[2], and insurers often recommend responders[3]. Report the loss without undue delay and facts that could lead to third-party claims within a week[2].
4. **Read five clauses before you renew.** War and state attacks, outages, ransom, payment fraud and fines. BIS and IAIS staff find that policy terms remain ambiguous[4].
5. **Size the cover from your measured recovery time.** The GDV model pays an agreed daily rate after a time deductible, for the agreed indemnity period only[2]. Set that period from the restore time you measured, as in the ransomware sheet.

## Answer the questionnaire

1. **Who answers?**
   IT or security answers the technical questions, finance the revenue and payment ones. If a representative concludes the contract for you, their knowledge counts as well as yours[2].
2. **What exactly is asked?**
   Mark scope words such as all, remote and admin. One German insurer asks about MFA for all remote access and for admins, EDR, patches within four weeks, flaws scored CVSS 8.0 or higher handled without delay and a yearly restore test of all backups[5]. A US form also asks about email filtering and MFA for webmail[6].
3. **Is it true for every system?**
   Check exports, not memory: MFA reports, EDR coverage, patch compliance, backup and restore logs. Describe any exception in writing, and keep a dated copy of the form with the exports.
4. **Report changes during the year.**
   Don't drop a control you reported without the insurer's consent, and report any increase in risk without undue delay[2], such as an expired EDR license.

## What a policy usually pays for

The GDV model terms are non-binding and insurers may deviate from them[2], so check each line against your own wording.

### Usually covered

- **Response costs.** Forensics, legal advice, notification, call center and PR, often through the insurer's providers[4,7].
- **Data restoration.** Restoring affected data to its earlier state and removing malware[2].
- **Business interruption.** Lost profit and running costs while systems are down[2].
- **Liability.** Defending and paying third-party claims, including data protection claims up to a sublimit[2].

### Only if you buy it, often sublimited

- **Ransom.** Excluded in the GDV model[2]; BaFin lets insurers bundle it with cyber cover[8].
- **Supplier outages.** Dependent business interruption isn't in every policy and is often limited to named providers[4].
- **Payment fraud.** Few cyber insurers cover it directly, mostly with sublimits[4]; the GDV points to fidelity insurance (Vertrauensschadenversicherung)[9].
- **Non-malicious failures**, such as a faulty update. The GDV model's triggers are attacks, unauthorized access, interference, malware and data protection breaches[2].

### Usually excluded

- **War and state attacks**, including war by digital means and state attacks that impair critical infrastructure[2].
- **Outages** of power, telecom and internet networks, and of a provider's service where they hit availability[2].
- **Fines and penalties**, unless agreed and insurable[2,10].
- **Contractual liability** beyond the law, **betterment** and **breaches that began before the policy**, unless retroactive cover was agreed[2].

## What changed in 2026

- **BaFin restated its ransom insurance rules.** The 1 April 2026 circular keeps the conditions: cover bundled only with cyber insurance, for a year at most, with duties to keep it secret and report to the police[8].
- **Fines in Germany: assume no cover.** Aon and A&O Shearman advise this until the law is clarified; defense costs can be covered[10].
- **Cover may tighten.** EU supervisors warn of stricter underwriting and more exclusions[11]; firms that can't fix flaws may become less insurable[4].

## When an incident starts

1. **Call the insurer's hotline at once.**
   Use the policy's crisis line and providers, and follow the insurer's reasonable instructions. Agree with the insurer before hiring your own responder or PR adviser[2], and get that in writing.
2. **Contain, but leave the damage in place.**
   Leave the damage scene unchanged until the insurer agrees, and document changes you can't avoid[2]. Isolate rather than wipe, as in the incident response sheet.
3. **Don't admit liability or settle.**
   An admission or settlement without the insurer's consent binds it only as far as the claim existed anyway[2].
4. **Count the loss from day one.**
   Log downtime, overtime, extra costs and lost orders per day. A month after reporting, you can claim an interim payment of the minimum amount owed so far[2].
5. **Ask the insurer before paying a ransom.**
   The GDV model excludes ransoms and pays nothing where sanctions stand in the way[2]. The ransomware sheet covers screening and the decision.

## Read these clauses in your wording

- **Territory.** The GDV model covers sites and systems you run yourself only in Germany unless extended, and third-party claims only when brought in EEA states under their law[2].
- **The war clause.** Since 31 March 2023, Lloyd's has required its standalone cyber policies to exclude state-backed attacks that significantly impair a state[12]. LMA5564A excludes every state cyber operation[13]; LMA5567A keeps cover for systems outside the impacted state[14].
- **Limits.** Sublimits count toward the main limit, which is also the annual maximum, and related incidents from one cause count as one[2].
- **Unpatched flaws.** The GDV model bars running systems with known flaws without extra safeguards[2]. Chubb allows 45 days after a CVE is published, then shifts more of the loss to you at 46, 90, 180 and 365 days[15].
- **Widespread events and failures.** Chubb, for one, sets separate limits for supply chain exploits, zero-days and cloud outages[15]. Test them against a case like the July 2024 CrowdStrike update, which cost Fortune 500 companies an estimated $5.4 billion[4], and ask about system failure: one loss event in four in Munich Re's claims is non-malicious[16].

## What you can skip

- **Chasing a perfect external security rating.** Underwriters also use outside ratings[4], so fix what they flag, but a claim turns on what you answered and kept up.
- **The highest limit on offer.** Small sublimits for ransom, outages and fraud make a large limit pay less than it looks.
- **Every service the insurer bundles in.** Many insurers offer consulting and risk management support[7]. Use what closes a gap in your controls.

## Mistakes that cost the most

- **Answering yes for all when one system is missing.** One VPN, admin or service account without MFA makes all untrue. If you claim measures that aren't in place, the insurer may not have to pay any claims[7].
- **Starting the renewal too late.** The GDV model renews for a year unless cancelled at least three months before expiry[2]. Start four months ahead.
- **Assuming other policies cover cyber.** Property and business interruption policies may give some cyber cover or exclude it[7].

## What this looks like at your size

### Small team, no security staff

- Have your IT provider sign off each answer.
- Check the policy's duties with your IT provider.
- Use four-eyes approval and call-backs for payments[9].

### Growing, with IT or security staff

- Give each answer an owner and evidence.
- List the providers whose outage would stop you, as in the third-party risk sheet, and check how the policy treats them.
- Rehearse a tabletop with the insurer's panel firm.

### Enterprise or regulated

- Have legal review the war, territory and fines clauses.
- Align notice duties with the EU security laws sheet.
- Agree who decides on a ransom, as in the ransomware sheet.

**Version history**

| | |
|---|---|
| **5 Nov 2026, version 1.0** | Published after a copy edit and a source-by-source fact check, which narrowed 8 statements to what the GDV model terms and other sources say. |

**Sources**


1. VVG, §§ 19 and 21. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
2. AVB Cyber: model terms for cyber risk insurance. GDV, Feb 2024. gdv.de
3. Guidance for organisations considering payment in ransomware incidents. NCSC (UK) with ABI, BIBA and IUA, 14 May 2024. ncsc.gov.uk
4. Cyber insurance unpacked: the corporate digital safety net. BIS FSI and IAIS, 17 Jun 2026. bis.org
5. Pro Cyber questionnaire (insurer's form). Markel, Jun 2025. content.markel.com
6. Smart Cyber application, v3.2 (insurer's form). Corvus Insurance, Sep 2024. help.corvusinsurance.com
7. Cyber insurance guidance. NCSC (UK), 6 Aug 2020. ncsc.gov.uk
8. Rundschreiben 01/2026 (VA): Lösegeldversicherungen. BaFin, 1 Apr 2026. bafin.de
9. Voice-Cloning und KI-Avatare. GDV, updated 12 Aug 2026. gdv.de
10. The Insurability of Cyber Fines (broker and law firm report). Aon and A&O Shearman, Feb 2026. assets.aon.com
11. Joint Committee update on risks and vulnerabilities, autumn 2026. ESAs, 23 Sep 2026. eiopa.europa.eu
12. Market Bulletin Y5381: state backed cyber-attack exclusions. Lloyd's, 17 Aug 2022. assets.lloyds.com
13. LMA5564A War and Cyber Operation Exclusion No. 1. LMA, 18 Jan 2023. lmalloyds.com
14. LMA5567A War and Cyber Operation Exclusion No. 4. LMA, 18 Jan 2023. lmalloyds.com
15. Cyber endorsements (product factsheet). Chubb (Germany), Nov 2021. chubb.com
16. Cyber insurance: risks and trends 2026 (insurer report). Munich Re, 25 Mar 2026. munichre.com