De prijs van gisteren voor het cyberrisico van morgen

Waarom een soft market geen bewijs is dat het tail risk is afgenomen

De prijsdruk in de cybermarkt houdt aan. In het tweede kwartaal van 2026 daalden de wereldwijde cybertarieven gemiddeld met 4 procent; het was het twaalfde kwartaal op rij waarin de tarieven daalden. Marsh (2026) schrijft dit toe aan stabiele capaciteit en aanhoudend sterke concurrentie. Aon (2026) ziet dezelfde soft market, maar wijst tegelijk op de toenemende severity van ransomwareclaims, AI-enabled attacks, privacyrisico's en kwetsbaarheden in digitale supply chains. Het Financial Stability Institute (FSI) en de International Association of Insurance Supervisors (IAIS) benadrukken in een gezamenlijke publicatie dat cyberincidenten in snelheid, schaal, verfijning en systemische impact toenemen (FSI en IAIS, 2026). Dat roept een ongemakkelijke vraag op: weerspiegelt de premie de onderliggende verliesdistributie, of vooral de hoeveelheid kapitaal die op dat moment een bestemming zoekt?

S. White MSc is Senior Technical Underwriter bij Hiscox Benelux.



Een lagere marktprijs hoeft niet onjuist te zijn. Betere cybersecurity controls, strengere underwriting en professionelere incident response kunnen zowel de frequentie als de schadelast verlagen. Extra capaciteit kan bovendien de protection gap verkleinen. Maar een gunstige recente loss ratio bewijst niet dat de tailscenario's minder zwaar of minder gecorreleerd zijn geworden. In cyber kunnen de marktcyclus, de schadeklok en de dreigingsklok uiteenlopen.

DRIE KLOKKEN, ÉÉN PREMIE

De kapitaalklok tikt per kwartaal: groeidoelstellingen, beschikbare capaciteit, herverzekeringskosten en concurrentie werken snel door in pricing. De schadeklok loopt trager. Claims moeten worden gemeld, ontwikkeld en afgewikkeld voordat portefeuille-ervaring betrouwbaar zichtbaar wordt. De dreigingsklok loopt sneller dan beide. Aanvallers veranderen hun werkwijze zodra bepaalde controls breed worden ingevoerd; nieuwe technologie verandert tegelijkertijd aanval, detectie en herstel.

Cyberrisico is daarom niet-stationair: de kansverdeling blijft niet gelijk door de tijd. Opeenvolgende portefeuillejaren voldoen dus niet vanzelfsprekend aan de klassieke i.i.d.-aanname: *independent and identically distributed*. Een portefeuille uit 2023 en een ogenschijnlijk vergelijkbare portefeuille uit 2026 kunnen een andere conditionele frequentie- en ernstverdeling hebben, ook wanneer omzet, sector en verzekerde limieten nauwelijks veranderen. Historische data blijven waardevol, maar hun halfwaardetijd is kort en structurele breuken moeten expliciet worden meegewogen. FSI en IAIS (2026) noemen pricing en accumulatie dan ook kernuitdagingen voor een duurzame cybermarkt.

HET LICHAAM VAN DE VERDELING IS NIET DE STAART

Voor veelvoorkomende schade blijft portefeuille-ervaring onmisbaar. Phishing, business email compromise, datalekken en ransomware geven informatie over frequentie, gemiddelde schadelast en de werking van controls. De verzekerde claims zijn echter een gefilterde versie van de onderliggende economische verliezen. Risicoselectie, eigen risico's, limieten, sublimieten, polisdefinities en uitsluitingen bepalen wat in de dataset verschijnt en waar bedragen worden afgekapt. De data bevatten daardoor selectie-effecten, truncatie en censurering.

Een dalende loss ratio kan meerdere oorzaken hebben: een werkelijk verbeterd risicoprofiel, een gewijzigde portefeuillemix, beperktere dekking, hogere retenties of eenvoudigweg het uitblijven van een accumulatiegebeurtenis. Vooral de staart blijft schaars geobserveerd. Daar spelen naast procesonzekerheid, de normale willekeur van schade, ook parameter- en modelonzekerheid: we weten niet precies welke distributie van toepassing is en hoe snel die verandert. Een paar rustige jaren kunnen de centrale verwachting bijstellen, maar identificeren de tailparameters niet betrouwbaar.

AI vergroot deze onzekerheid. Dezelfde technologie kan aanvallen automatiseren en kwetsbaarheden sneller vinden, maar ook detectie, patching en incident response verbeteren. Wie per saldo voordeel krijgt, staat niet vast. De European Systemic Risk Board (2026) waarschuwt dat frontier AI models op korte tot middellange termijn de snelheid, schaal en verfijning van aanvallen kunnen vergroten. Dat is niet alleen extra procesvariatie rond een stabiel gemiddelde, maar een mogelijke structurele verschuiving van de distributie.

ACCUMULATIE IS VERBORGEN AFHANKELIJKHEID

Bij fysieke risico's kunnen we concentraties vaak op een kaart aanwijzen. Cyberaccumulatie loopt via gedeelde digitale afhankelijkheden door sectoren en landsgrenzen heen. Verschillende verzekerden kunnen gebruikmaken van dezelfde cloud service provider, identity provider, software library, managed service provider of endpoint security tool. Een foutieve update (Crowdstrike), langdurige storing (AWS US-East-1), breed uitgebuite kwetsbaarheid (Log4Shell), een zero-day in gedeelde bedrijfssoftware (MOVEit) of wijdverspreide malware (NotPetya) vormt dan een gemeenschappelijke oorzaak voor grootschalige en gelijktijdige claims.

Onder normale omstandigheden kunnen de onderlinge correlaties laag lijken. In de staart kan juist sterke tail dependence ontstaan: onder stress neemt de afhankelijkheid toe. Diversificatie naar sector of geografie valt dan weg op het moment dat we haar het hardst nodig hebben. Het relevante scenario is niet alleen één uitzonderlijk grote claim, maar een groot aantal op zichzelf normale polissen dat tegelijk reageert. Munich Re (2026) wijst eveneens op de dynamiek van zowel kwaadaardige als niet-kwaadaardige incidenten en op de kwetsbaarheid van digitale ketens.

ÉÉN TECHNISCHE PRIJS, TWEE INFORMATIEBRONNEN

De oplossing is niet om historie terzijde te schuiven of elke polis uit voorzorg duur te maken. Conceptueel bestaat de technische prijs uit de verwachte attritionele schadelast plus een risk load voor tail risk, accumulatie, kapitaalkosten en modelonzekerheid. Voor het lichaam van de distributie kan recente portefeuilledata worden gebruikt; voor de staart kunnen scenarioanalyse, afhankelijkheidsdata en stresstests worden ingezet.

Scenario's vervangen statistiek niet, maar vullen het gebied in waar waarnemingen schaars zijn. Ze hoeven niet te worden voorzien van kansen die preciezer lijken dan onze kennis rechtvaardigt. Hun functie is de grenzen van capaciteit, herverzekering, polisstructuur en risk appetite zichtbaar te maken. Ook het verschil tussen de technische prijs en de commerciële marktprijs is managementinformatie. Een verzekeraar kan tijdelijk bewust onder de technische prijs schrijven, maar de afwijking hoort expliciet, begrensd en bestuurbaar te zijn, niet verstopt in een optimistische extrapolatie van recente loss ratio's.

Ook modelaannames hebben een houdbaarheidsdatum nodig. Cloudafhankelijkheden, aanvalspaden, hersteltijden en de effectiviteit van controls moeten periodiek worden herijkt. Threat intelligence, schadegegevens en portefeuilleafhankelijkheden horen daarom in één doorlopende feedback loop samen te komen. Zo kunnen overtuigingen geactualiseerd worden met nieuwe ervaring, zonder te doen alsof het meest recente verleden de enige mogelijke toekomst beschrijft.

CONCLUSIE

Nieuw kapitaal is niet de vijand van een duurzame cybermarkt. Het kan dekking toegankelijker maken en innovatie financieren. Maar extra capaciteit verkleint de gemeenschappelijke afhankelijkheden niet en maakt een niet-stationair risico niet stationair.

Cyber blijft verzekerbaar, mits we marktprijs en technische prijs, lichaam en staart, en proces- en modelonzekerheid van elkaar blijven onderscheiden. Historische portefeuilleprestaties zijn een noodzakelijke informatiebron, maar geen veilige automatische projectie. In cyberverzekering is de grootste fout niet dat we het verleden niet volmaakt voorspellen, dat is bekend, maar dat we geneigd zijn de premie te laten bepalen door beschikbaar kapitaal en historische data zonder rekening te houden met materiële verschuivingen in de dreigingsrealiteit. ■

Bronnen

– Aon (2026). *Cyber and E&O: Market Remains Soft but Volatility Grows.*
– European Systemic Risk Board (2026). *Frontier AI models could strain cyber resilience in the financial system.*
– Financial Stability Institute & International Association of Insurance Supervisors (2026). *Cyber insurance unpacked: the corporate digital safety net. FSI Insights No. 75.*
– Marsh (2026). *Global Insurance Market Index, Q2 2026.*
– Munich Re (2026). *Cyber insurance: Risks and trends 2026.*

