

# Seeing Risk from the **Outside In**

## Why cyber risk assessments need fewer assumptions – and more precision.

The global cyber insurance market finds itself at a moment of unmatched opportunity, with significant growth potential, ever-increasing understanding of risk, and a cyber threat landscape that makes the need for risk assessment, mitigation, and insurance more prevalent than ever before. Yet the insurance industry faces challenges in driving new market expansion. Zywave recently had the opportunity to sit down with Jonas Schwade, CEO of cysmo Cyber Risk GmbH, who shared his thoughts on why insurers and brokers need to craft a common language on cyber risk to better connect with potential clients and how outside-in scanning technology designed for the cyber market can foster trust in insurance partnerships.



As CEO of cysmo Cyber Risk, **Jonas Schwade** drives innovation in cyber risk assessment with the market-leading “Outside-in” technology, redefining how insurers approach cyber risk. With deep expertise in cyber risk and insurance, he regularly speaks at global conferences, shaping the future of cyber insurance through cutting-edge solutions. In addition, he supports insurtechs as an advisory member, fostering innovation and collaboration within the industry.

**Zywave:** Can you share how your path brought you to the insurance world?

**Jonas Schwade:** I've always worked close to the insurance industry — but it was the early days of cyber where things truly clicked. We saw insurers trying to evaluate digital risk using tools built for IT teams, not underwriters. And we thought: there must be a better way.

So we brought together people from across the spectrum — underwriters, security experts, white-hat hackers, data analysts — all with the same goal: to translate cyber risk into something insurers can understand, work with, and trust.

That's what shaped our platform from the start: not just coverage-focused, but under-writing-ready. Not just technical — but truly insurance-native. That was back in 2017 in Germany.

**Zywave:** In 2017, cyber insurance in Germany was just gaining traction. What was the landscape like?

**Schwade:** At that time, there was a lot of energy, but not much structure. Everyone saw the opportunity — few knew how to act on it.

Back then, we sat in meetings where people couldn't explain the difference between a firewall and a phishing link. And suddenly they were asked to underwrite it. That's when we realized: without the right language, cyber can't scale.

So we created a platform that scans from the outside in — just like an attacker would — and translates complex signals into clean, actionable insights insurers can actually use.

**Zywave:** Has the industry found that common language yet?

**Schwade:** Not fully. Cyber is still intimidating to many brokers and clients. Especially in the SMB segment, which is key to unlocking growth. The education gap on both sides and the fear to talk about technical details still slows things down.

That's why real-time visibility and simple analogies help — like the open-window metaphor. But beyond that, we also deliver potential loss estimates. That changes the conversation entirely — from theoretical to tangible.

**Zywave:** Where's the opportunity for real growth in the cyber market?

**Schwade:** It's tempting to chase large enterprise deals — but sustainable growth starts with scale. And that means mid-sized businesses.

They're under increasing pressure: from regulators, from partners, from customers. Frameworks like the Digital Operational Resilience Act (DORA) in Europe or U.S. Securities and Exchange Commission (SEC) scrutiny in the U.S. are pushing them to act. And when procurement starts asking about insurance and cyber hygiene — you know the market is shifting.

For brokers and carriers, that's a chance to evolve. Not just by offering a policy — but by becoming a partner in resilience.

**Zywave:** Do regional differences affect how cyber insurance is sold?

**Schwade:** Definitely. We've analyzed millions of companies across different geographies — and no two regions behave the same. You will see technological differences, which makes sense. A company from the LATIN market has other challenges compared to a company from Europe.

That's why you can't sell cyber in Montreal the same way you do in Munich or Tokyo. Whether it's tech stacks, threat exposure, or policy structures — local knowledge matters. Which is why insurers need risk intelligence that adapts, not templates that generalize.

**Zywave:** What convinces clients of the value of a cyber policy?

**Schwade:** Most clients don't fear cyber risk until they see it reflected back at them. It's important to show them the value of the policy before they need it.

If you think about a fire. In case of a fire everyone knows to call 911. In a cyber incident? That's where insurance steps in – not just to reimburse, but to coordinate expert response.

I see a lot of companies not only deciding to buy a policy because of the money but more to have access to a network of experts who could help them in case of an event

We show exposure in real time. And we don't just stop at risk scores — we estimate what a breach could cost. That's when things get real. Not in theory. In dollars. And in downtime.

**Zywave:** How has the insurance industry adopted scanning tools like yours?

**Schwade:** There's been a clear shift. Carriers want data, but they want it to make sense. And more and more players start to understand where the actual benefit of data comes into play.

What is more important than ever these days is that the data has to be accurate. Reliable. Fast. And tailored to insurance — not IT. That's been our guiding principle since day one.

We've seen it firsthand. Insurance companies that have had negative experiences with scan reports full of false positive signals that lead to frustration on every side. If you show them on the other side how accurate data can actually reveal companies at risk before there is a cyberattack and that clients are happy about these insights. That kind of insight turns skepticism into conviction.

**Zywave:** What's the biggest risk of using noisy cyber tools in insurance?

**Schwade:** Loss of confidence — on both sides.

If you present flawed reports to clients, you risk credibility. If you rely on noisy data for pricing, you risk accuracy.

Insurance runs on trust. And trust doesn't survive uncertainty. That's why we focused so heavily on eliminating false positives — because every error has a cost.

**Zywave:** What happens when a client sees false positives in a cyber report?

**Schwade:** They start questioning more than just the report. They question your process, your premiums, your value.

We've seen it before: "If this isn't even our system — what else is wrong?" "Are these wrong signals influence our pricing?" That doubt sticks. And it's hard to earn back. Precision is more than technical hygiene — it's a trust guarantee.

**Zywave:** What's the future of pricing in a volatile cyber landscape?

**Schwade:** The market is still young and everybody in this market is collecting experiences. Overcoming the uncertainty, especially on the client side is not always easy.

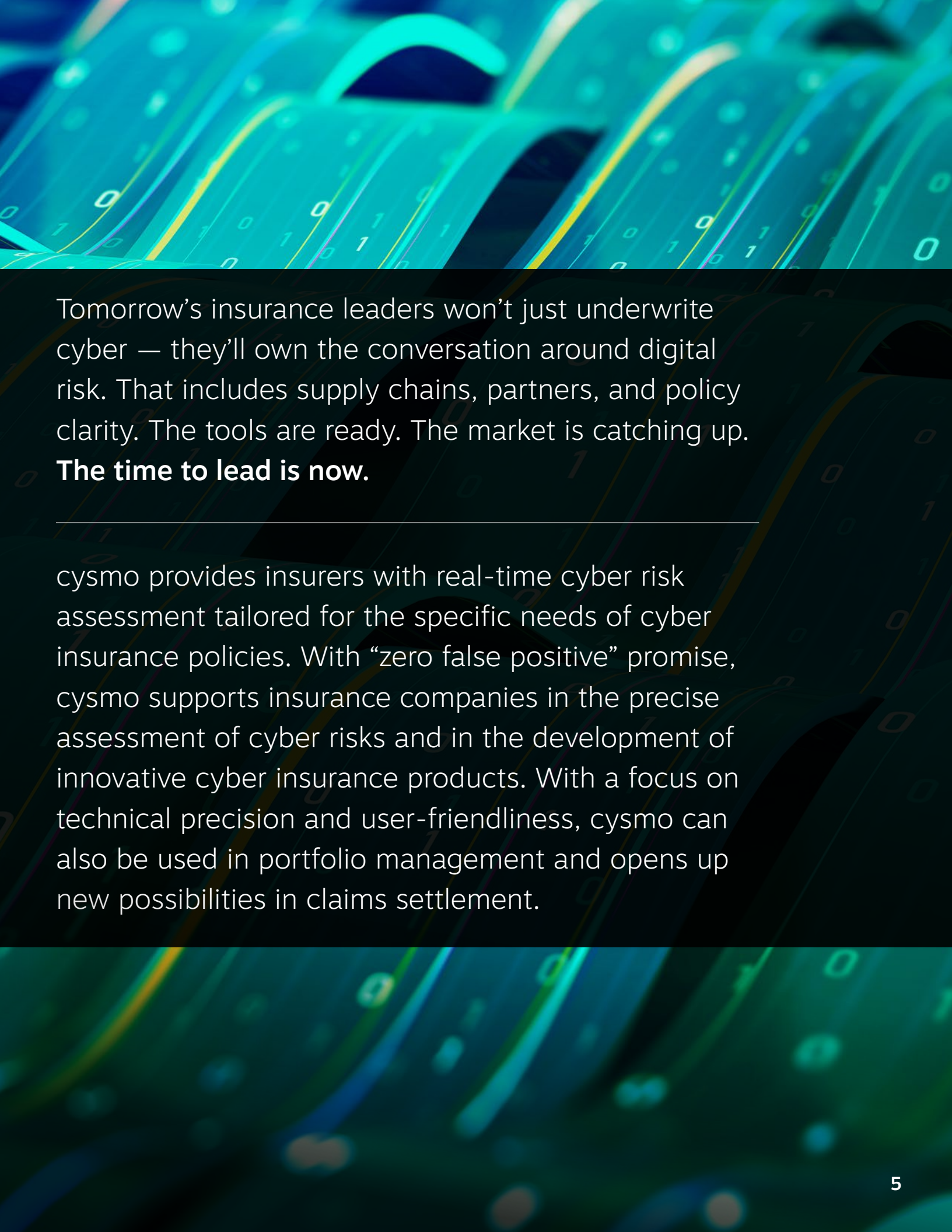
It's about transparency. Cyber risk evolves daily — even if the insured company doesn't change.

It needs to be dynamic — but it also has to be explainable.

Clients understand that threats evolve. What they need is transparency: What changed? Why did the premium shift?

That's where platforms like ours help — not by locking in a price, but by providing clarity on how risk is shifting, even when the company itself hasn't changed.



The background of the slide is a vibrant, abstract digital illustration. It features a dark blue and teal color palette with glowing, flowing lines in shades of yellow, orange, and light blue. Scattered throughout are binary digits (0s and 1s) in various sizes and colors, giving the impression of data streams or digital pathways. The overall effect is one of high-tech, futuristic energy.

Tomorrow's insurance leaders won't just underwrite cyber — they'll own the conversation around digital risk. That includes supply chains, partners, and policy clarity. The tools are ready. The market is catching up.  
**The time to lead is now.**

---

cysmo provides insurers with real-time cyber risk assessment tailored for the specific needs of cyber insurance policies. With “zero false positive” promise, cysmo supports insurance companies in the precise assessment of cyber risks and in the development of innovative cyber insurance products. With a focus on technical precision and user-friendliness, cysmo can also be used in portfolio management and opens up new possibilities in claims settlement.