QBE Insurance

Cyber only knows change

Cyber insurance market's maturity evident in the ability to adapt in the face of constant change

The global cyber insurance space experienced significant change in a short time, requiring market players to quickly identify emerging trends and react responsibly. The industry might be considered a nascent one, but the constant pace of evolution makes for a savvy, and increasingly mature market.

"Cyber is often described as an immature product and I want to flip the script on that," said Desirée Spain, Global Head of Cyber Underwriting Management for QBE, in a recent interview with Zywave. "When a product is considered 'mature,' it usually means innovation has slowed and it's become a commodity. But cyber is different – the technology and threat landscape evolve so quickly that the risk is constantly shifting. It's never going to be static."

She added, **"cyber only knows change,** so we've had to stay agile," said Spain. "We've built a responsive process – one that lets us quickly identify emerging risks, develop coverage, and adapt our underwriting. In that sense, while the product itself may not be mature, the market's ability to evolve around it absolutely is."

What makes for a mature market? According to Spain, indicators include stable pricing and underwriting models, an established regulatory framework, and widespread market adoption.

"These areas are still evolving," said Spain. "Market adoption – especially internationally, but also in the U.S. – relies on continued education and dialogue. Brokers and buyers are already engaging with the risk, but deeper understanding and confidence in the product's value will help drive broader uptake."

The cyber market's unique role in covering an evolving risk, particularly at a time of intense competition, offers insurers the chance to continuously refine their product offerings.

Desirée Spain
QBE Global Head of Cyber Underwriting

"Unlike many products, cyber requires us to move quickly," said Spain. "We need a solid understanding of the risk, stay alert to how it's shifting, and assess what claim trends mean for coverage. When we spot a gap, we aim to respond with a solution that matters."

Insurers examine the exposure, evaluate claim patterns, and monitor the risk environment, she added. It's an opportunity for the cyber market to shine on underwriting amid competition.

A few of the latest trends in cyber, particularly non-breach privacy litigation and artificial intelligence, offer a glimpse of the market's ability to react thoughtfully, according to the QBE executive.

Privacy litigation over alleged wrongful collection of data and business use of pixel tracking technology saw a major uptick over the past two years. Plaintiffs have increasingly applied older federal privacy laws and state wiretapping laws to file complaints over collection of consumer data via websites.

"It caught the market – and clients – off guard," said Spain. "We've seen a wave of claims, but the industry is starting to better understand what's driving wrongful collection issues and how clients can reduce that risk."

That in-depth look into the causes of cyber claims fuels a feedback loop to help insureds improve their cybersecurity posture, as well as refine the underwriting process.

"We've now seen enough of these claims to start asking smarter questions and offering clearer guidance," said Spain. "We want to understand how data is collected, what privacy and opt-in policies are in place, what types of user information are gathered, and how that's communicated – through things like cookie banners, terms of use, and consent flows. It's about making sure clients are not only compliant, but also transparent and well-prepared."

The impact of AI on cyber risk, both external and internal, has insurers eyeing an emerging risk that could ultimately impact several different lines of business.

"With AI, we've spent a lot of time asking whether it's introducing new risks or simply amplifying existing ones," said Spain. "There's ongoing discussion around how to design a product that truly addresses exposures unique to AI – and where we, as insurers, can add real value."

Besides self-reflection, insurers continually enhance their methods for precisely assessing clients' exposure to cyber loss. Detailed applications questions remain a key part of the underwriting process. As threats shift, questions need to follow suit – even in a softer market.

"We're getting to a point where more targeted underwriting questions are essential," said Spain. "For example, a client might have an EDR tool in place – which is great for spotting malicious activity and responding quickly – but how and where it's deployed across the network really affects its effectiveness. If it's not applied consistently, it can leave critical blind spots."

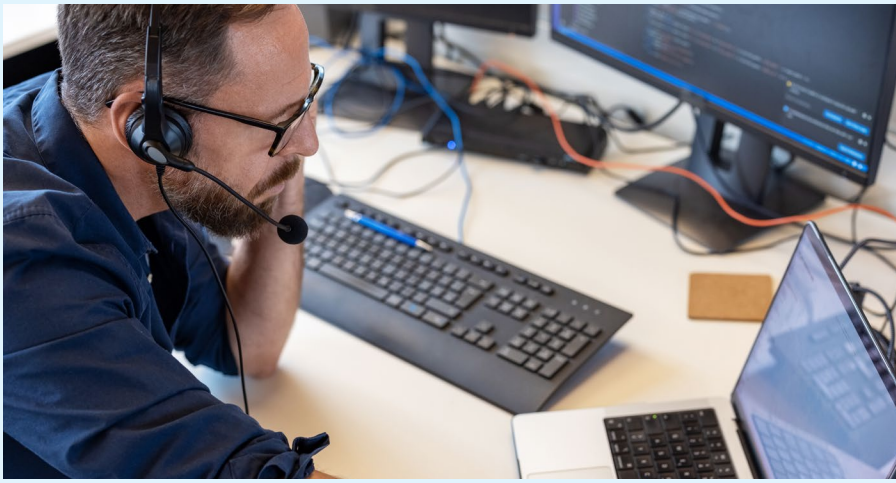
"We often see claims from clients who have EDR in place, but haven't rolled it out across their entire environment," said Spain. "Sometimes it's only installed on endpoints, while servers are left exposed – creating vulnerabilities. In other cases, the client may have purchased an EDR

solution but skipped some of the advanced features that offer the kind of protection we'd typically expect. These gaps are leading to claims, which is why it's so important for us to dig deeper and ask more targeted questions during underwriting."

"It's not just EDR we need to ask about – firewalls and MFA deserve closer scrutiny too," said Spain. "We should be asking what types of external devices and firewalls are in use, especially those known to be frequently targeted, like Fortinet, SonicWall, or certain VPN products. Threat actors like Akira often exploit vulnerabilities in these areas. And when it comes to MFA, simply having it isn't enough – we need to know if it's enforced, what type is used (SMS vs. tokens), and what controls are in place to prevent bypass. These details can make a real difference in understanding a client's risk posture."

The insurer's involvement in supporting insureds doesn't end with the binding of a policy. Insurers have expanded their proactive services to include targeted threat intelligence, external scanning, and governance guidance to help insureds understand risk mitigation better.

"A security assessment helps us evaluate the risk, but it also gives clients clearer insight into their own exposure," said Spain. "The global cyber insurance market should take pride in its growing role as a force for good in cybersecurity. By driving better risk practices and offering proactive support, insurers are not only protecting organizations – they're contributing to a safer digital society. That impact should inspire us to push for broader market penetration."



"The cyber market has evolved tremendously – both in terms of product innovation and underwriting sophistication," said Spain. "We've made meaningful progress, and it's exciting to see how far we've come."

QBE Insurance