



cyber insurance into an essential cyber resilience partner. Market data further contradicts the hyperbole: while cyberattacks continue to grow, losses have not increased proportionally, and the pace of cyber premium growth has stabilized. The discipline of underwriting, coupled with exclusionary language and pricing tools, has allowed insurers to better manage catastrophic cyber exposures. There is broad industry consensus that catastrophic cyber losses are challenging but generally remain manageable when insurers are allowed to use the full suite of risk management tools.

Nevertheless, systemic risk remains a legitimate concern. Critical infrastructure sectors, frequent targets of nation-state and terrorism-motivated cyberattacks, are not always sufficiently homogeneous for traditional risk pooling, and catastrophic attacks can challenge conventional notions of insurable risk. Regulatory fragmentation also complicates insurability; excessive or unpredictable rules can create uncertainty and reduce capacity. New industry exclusions and endorsements under development aim to better define government-related risks, and discussions about potential public private partnerships continue, though many believe it is premature to design a government program before market needs are fully understood.

Operational resilience remains central. Insurers are strengthening their own cyber defenses, improving third party oversight, and conducting more rigorous testing and crisis communication exercises. Regulatory alignment, particularly around incident reporting triggers and information sharing practices, would further reduce friction in high pressure moments. Proportionality matters here: one-size-fits-all requirements may impose costs misaligned with risk, while flexible, outcomes-based expectations better reflect the diversity of insurers and markets.

Building expertise is equally important. Cyber risks require specialized technical capabilities, both within companies and among supervisors. Smarter analytics, improved data management, and more consistent supervisory expertise will improve cyber resilience throughout the system. Cybersecurity will remain a central challenge for insurers as digital risks continue to evolve. But the evidence is clear: insurers are not the weak link, they are actively reinforcing the chain. Through disciplined underwriting, responsible AI adoption, stronger governance, and full lifecycle support, insurers are transforming perceived vulnerabilities into safety nets that protect policyholders and strengthen the broader digital economy.