Cyber Insurance Premiums Are Soaring — And So Are Your Risks

By Michael C. Maschke, Sharon D. Nelson, Esq., and John W. Simek

The global cybersecurity insurance market is about to explode. A new forecast predicts it will more than double by 2030 — jumping from roughly $16.5 billion today to $32 billion in just five years. That's a 14% annual growth rate, which in insurance terms is rocket fuel.

Why the sudden surge? And, more importantly, why should law firms (and their clients) care?

Breaches, Ransomware, and the Regulatory Tsunami

Ransomware is now a multibillion-dollar criminal industry. Breaches at law firms, health care systems, and Fortune 500 companies dominate headlines. And regulators aren't sitting this one out. Between Europe's GDPR, the NIS2 directive, and the U.S.'s expanding patchwork of state privacy laws, the compliance stakes have never been higher.

For many businesses, insurance is becoming the only realistic safety net. Cyber policies are no longer "nice to have." They're fast becoming a requirement — by boards, clients, and regulators alike.

The Insurance Industry Is Playing Catch-Up

Insurers are scrambling to adapt. Legacy carriers like Chubb, Travelers, and Liberty Mutual are bundling cyber coverage with traditional policies, while also forming alliances with cybersecurity firms like BitSight and SecurityScorecard. The idea is to combine actuarial data with real-time threat intelligence to price policies more accurately — and to push clients toward better security before a claim ever lands.

Why does this matter? Because underwriting cyber risk is notoriously difficult. There aren't decades of claims data to lean on, and threat actors innovate faster than most corporate defenses. Expect carriers to continue tightening their underwriting requirements — think mandatory MFA, endpoint detection, and documented incident response plans. If you're advising clients (or running your firm), that shift is coming for you, too.

North America remains the 800-pound gorilla of cyber insurance, accounting for nearly 70% of global premiums. But Asia-Pacific is the fastest-growing region. Rapid digitization, combined with new regulatory mandates, is pushing organizations to seek coverage at record speed. Expect more global carriers to establish a presence in Asia-Pacific over the next few years.

Here's the uncomfortable truth: most businesses still don't have cyber coverage at all. And even when they do, policy limits are often laughably low compared to the potential fallout of a serious incident.

Global cybercrime losses in 2024 were estimated somewhere between $1 trillion and $9.5 trillion (yes, trillion with a "T"). Premiums? A fraction of that. The gap between losses and coverage is staggering — and attackers aren't slowing down.

Why Lawyers Should Care

For law firms, this isn't just another industry statistic. Cyber insurance directly impacts your risk profile and the advice you give to clients:

- Your firm's coverage: If you're still treating cyber insurance as optional, stop. Client data, privileged communications, escrow accounts — all are prime targets. As an added incentive, clients may require that you have minimum cyber coverage. Coverage isn't just about reimbursement; it's about access to breach coaches, forensics, and PR resources you'll desperately need when things go wrong.
- Client counseling: Whether you handle deals, litigation, or employment matters, your clients' cyber risks are intertwined with your own. Asking "Do you have cyber insurance?" isn't prying — it's prudent.
- Contract negotiations: Cyber insurance is increasingly appearing in deal terms. Representations, warranties, and indemnification clauses often hinge on it. Know the basics — or risk leaving clients exposed.

The Bottom Line (and the To-Do List)

Cyber insurance is growing because cyber risk is growing — fast. By 2030, the market will likely be twice its current size and still struggling to keep pace with increasingly sophisticated attackers.

Don't wait for the next ransomware headline. Review your firm's cyber insurance policy this quarter — confirm the coverage limits, exclusions, and incident response support. Then encourage your clients to do the same.

When (not if) the next significant breach happens, the only thing worse than being attacked is realizing your coverage won't cover what matters.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com*