

Cyber Insurance Is Not a Cybersecurity Strategy

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

Cyber insurance has officially gone mainstream.

According to the 2026 Travelers Risk Index, 70% of surveyed businesses now report purchasing cyber insurance, up seven percentage points from last year and the highest level since the survey began focusing on cyber risk in 2018. Among large businesses, adoption has reached 82%, while even half of small businesses now report having coverage.

That's encouraging news. Law firms should carry cyber insurance. The potential costs of ransomware, data breaches, business interruption, forensic investigations, regulatory actions, and litigation can quickly become enormous. But there's a danger in mistaking cyber insurance for preparedness for a cyberattack.

Insurance Isn't a Security Control

No law firm would buy fire insurance and then conclude it no longer needs smoke or fire-detection devices. Cyber insurance should be viewed the same way.

Policies can help absorb some of the financial consequences of an incident, but they don't prevent it. It won't stop an employee from entering credentials on a convincing phishing site, prevent an attacker from exploiting an unpatched server, or keep a compromised account from accessing confidential client information.

The Travelers survey offers some encouraging news on this front. Businesses are investing more heavily in firewalls, backups, employee screening, stronger onboarding and offboarding procedures, and multifactor authentication.

But significant gaps remain. Only 72% of respondents reported using multifactor authentication for administrative users. That means more than one-quarter still aren't applying one of today's most fundamental security controls to some of their most powerful accounts.

Then There's AI

Artificial intelligence makes the numbers even more interesting.

Nearly nine out of 10 respondents said AI is now used in their day-to-day operations. Yet only 59% said their organizations have formal practices governing employees' AI use. That's a 30-point gap between adoption and governance.

For law firms, that should sound familiar. Attorneys and staff have embraced tools like ChatGPT, Copilot, and other AI platforms remarkably quickly, often faster than firms can develop policies governing what information can be entered into these tools, which tools are approved, and how AI-generated work should be reviewed.

Cyber insurers are paying attention to these evolving risks. Firms should do the same.

Knowing that you have a cyber insurance policy is no longer enough. Firm leaders should understand what the policy covers, what it excludes, which security controls the firm represented were in place when applying for coverage, and what the policy requires when an incident occurs.

Test The Plan Before You Need It

One of the more revealing findings in the Travelers survey concerned incident response. While businesses are adopting more preventive security measures, fewer regularly conduct cyberattack simulations or test their incident-response plans. That's a missed opportunity.

A written incident-response plan may look great in a binder or on a server. The real test is whether the people named in it know what to do when an incident actually occurs.

Who calls the insurer? Who contacts breach counsel? Who has the authority to shut down systems? How will attorneys communicate if email is unavailable? Who communicates with clients? Does everyone know where the cyber insurance policy and emergency contact information are stored?

A tabletop exercise can expose these problems before an actual attacker does so.

Coverage Is Only Part of the Strategy

The growth of cyber insurance is a positive development. Cyber incidents can create significant financial exposure, and insurance has become an important part of managing that risk.

Insurance should be the financial backstop, not the cybersecurity strategy.

Law firms still need the fundamentals: multifactor authentication, tested backups, endpoint protection, security awareness training, vulnerability management, appropriate access controls, and a practiced incident-response plan. AI governance also belongs on that list.

Seventy percent adoption of cyber insurance sounds like progress, and it is. But after an attack, the number that matters isn't whether your firm checked the box to say it had a policy. It's whether the firm was prepared to use it.

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.