Your Cyber Insurance May Not Be Ready for Autonomous AI

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

Law firms have spent the past several years asking whether artificial intelligence will improve productivity. A different question is beginning to emerge.

What happens when AI starts making decisions on its own?

The next generation of AI isn't limited to drafting emails or summarizing documents. Autonomous AI agents can perform multi-step tasks, interact with third-party systems, execute transactions, and make decisions with minimal human oversight. These capabilities promise significant efficiency gains, but they also introduce risks that many organizations and their insurers are only beginning to understand.

According to recent reports, cyber insurers are increasingly scrutinizing how organizations deploy autonomous AI and whether existing cyber insurance policies adequately address the new exposures these systems create. The concern isn't simply that AI creates new cyber threats. It's that organizations may unknowingly introduce risks that fall outside the assumptions underlying their insurance policies.

AI Changes More Than Technology

Traditional cybersecurity focuses on protecting systems against unauthorized access, malware, ransomware, and data breaches. Autonomous AI poses a different challenge.

Instead of merely assisting employees, AI agents may be authorized to access client files, send communications, interact with financial systems, retrieve confidential information, or make operational decisions on the firm's behalf. The authorizations are not significantly different than permissions granted to apps on your smartphone to the data stored on your phone (personal and client). As organizations grant these systems greater authority, questions of accountability become significantly more complex.

If an autonomous AI agent exposes confidential client information, authorizes an inappropriate transaction, or makes a decision that causes financial harm, was it a cyber incident, a professional liability issue, or an operational failure?

The answer may not be as straightforward as existing insurance policies assume.

Governance Matters More Than Ever

For law firms, this is less about buying new insurance and more about implementing thoughtful governance.

Firm leadership should know where autonomous AI is used, what information it can access, what decisions it is authorized to make, and what safeguards are in place to prevent unintended actions. Just as importantly, firms should maintain meaningful human oversight for high-risk activities involving client data, financial transactions, or legal work product.

These questions increasingly mirror the cybersecurity conversations firms have already had about privileged access, vendor management, and cloud security. AI governance is becoming another component of enterprise risk management rather than a standalone technology initiative.

Don't Wait Until Renewal

Cyber insurance applications have become significantly more detailed over the past decade. Questions about multifactor authentication, endpoint detection, backups, and incident response planning have become commonplace as insurers have learned that these controls materially affect risk. AI governance may be next.

Organizations that can demonstrate clear policies, documented oversight, access controls, and responsible deployment of autonomous AI will likely be better positioned as underwriting evolves. Firms that cannot explain how AI operates in their environment may face additional scrutiny, coverage limitations, or difficult conversations after an incident.

Conversation Is Bigger Than Insurance

Whether cyber insurance policies ultimately change is almost beside the point.

The more important takeaway is that autonomous AI is compelling organizations to rethink risks. The same technology that promises greater efficiency also raises new questions about accountability, governance, and professional responsibility.

For law firms, AI should not be viewed as merely another productivity tool. It should be managed with the same discipline applied to any technology that can access confidential information or make decisions that affect clients.

Cyber insurance may eventually adapt to these new realities. The firms that succeed will be those that adapt first.

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.*