Cyberinsurance and Cyberattacks: Evolving Trends for Coverage in 2025

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

Cyberattacks continue to evolve as technology advances, and so do the methods by which attackers attempt to compromise business and personal email accounts, computer systems and cloud-based services. The introduction of artificial intelligence (AI) into attackers' processes and software has further fueled an already raging fire. Cloud service providers, like Google, are not immune either, with Google recently warning its roughly three billion users of advanced AI-driven phishing attempts and phone scams targeting Gmail accounts.

Law firms are struggling to keep up, with some more prepared to defend their information systems than others. Most are playing catch-up to a goal line that is constantly moving farther and farther away. Cyberinsurance carriers, having paid out substantial amounts of money in claims during the pandemic, are also evolving their business practices.

Cyberinsurance carriers are shifting towards a comprehensive policy approach, moving away from offering traditional policies that cover only immediate financial losses from cyber incidents, such as ransomware attacks and data breaches. Businesses need coverage from prevention to post-breach support and are starting to wake up to this realization.

The shift towards comprehensive coverage is a new trend in 2025, with businesses seeking coverage that addresses multiple layers of protection, including not only direct financial loss but also monitoring, assessments, training, and other cybersecurity protections that can be critical in mitigating potential threats.

Increasingly Popular Types of Coverage

It never hurts to be informed about the various types of policies available for your firm, especially when your cyber insurance coverage comes up for renewal. Cyberinsurance carriers are seeing a significant increase in demand for the following types of coverage areas:

Data Breach Coverage – covers costs related to a breach, including legal fees, notification fees, and services offered for affected individuals.

Business Interruption – covers loss of revenue of operations due to a cyberattack.

Cyber Extortion – financial reimbursement for businesses that fall victim to a ransomware attack.

Incident Response and Forensic Services – covers the costs of experts who respond and investigate a breach.

Reputation Management and Legal Expenses – covers public relations efforts and legal costs post-breach.

Cyberinsurance carriers are shifting to more comprehensive coverage to address the evolving landscape of cyber threats, covering a wider range of risks, as well as compliance requirements such as GDPR and CCPA that businesses must comply with. Additionally, they are recognizing the growing need for post-breach support, which companies require more than ever.

Understand that comprehensive policies don't come without added costs – let's not get ahead of ourselves. Insurance companies should NEVER be confused with charities. We expect that you already know that, to your consternation. Expect to see insurers start to switch to dynamic-based pricing models, dependent on the insured's risks or the likelihood of them experiencing a cyber incident within the coverage period. The one-size-fits-all pricing model has become outdated due to the increasing risk that businesses face from cyberattacks. Consequently, insurers are now using AI models to determine policy pricing for businesses. Are you groaning yet?

H**ow does this affect your firm?**

As insurers move toward AI models to dynamically determine premium pricing and overall coverability, these models ingest data from your applications and leverage real-time information from continuous monitoring tools, vulnerability scans, breach history, and even whether your employees have recently completed a cybersecurity awareness training course. The carriers may require that you implement certain software agents to perform the data collection that is fed to the AI model. Make sure that any transmitted data does not include any client confidential data.

What does this mean for your firm? More than ever, it's essential to be proactive in implementing cybersecurity measures, protections, and education. Because this data is now being evaluated by AI models to determine your business' risk, along with real-time vulnerability scanning results that insurers are rolling out, it has a direct correlation with your premium and whether it needs to be increased or lessened (hopefully), depending on how serious you are about protecting your firm's assets and client data from cyber threats.

With this potential added benefit, there is no time better than now to be proactive about your firm's cybersecurity posture and protections. When to begin this process? Immediately!

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*