Law Firms Taken Aback by the Impact of AI and the Rise of Exclusions on Their Cyberinsurance Policies

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

The Cyberinsurance World is Rocked by AI

That's a good thing – and a bad thing, especially for law firms. Artificial intelligence is very good at assisting insurers in assessing risk and reducing errors in the application process. In theory, the AI would help insurers pick the plan most suited to the customer's needs.

The downside is that AI can be problematic as a risk. You may even need to secure specific coverage if you're using it.

Hiding Anything from Your Cyberinsurance Carrier?

We often see law firms give answers to cybersecurity application questions that are, well, wrong. Sometimes they make mistakes in their answers, but sometimes they know they are giving an incorrect answer. Hence, the risk assessment done by the insurer might be a fairy tale. That could come home to bite the law firm in the event of an incident.

New this year: With Increasing rapidity, AI can now pore through all sorts of resources – online reviews, social media, SEC filings, and much more to get a more realistic picture of the insurance carrier's risk in insuring your law firm. The insurer could decline coverage or call you and ask you to explain your answers.

If you've been breached before, AI will find evidence of that too . . .

We're Sure You Never Considered Filing a Fraudulent Claim, But . . .

Something more extraordinary is now afoot. It may shock some readers to learn that AI has now attained a 77% accuracy rate for detecting fraudulent insurance claims. Shift Technology has processed over 77 million claims – the accuracy rate derives from the company's own usage of AI to uncover fraud.

Didn't mom always teach you it was better to tell the truth? In the era of AI, mom sure was right.

Ransomware: The Nemesis that Keeps on Coming

Boy oh boy, do we need our cyberinsurance. The average ransomware payment almost doubled from $812,000 in 2022 to over $1.54 million in 2023, according to *The State of Ransomware 2023* report by Sophos. Sound scary? Consider this – the average cost to recover from a ransomware attack escalated to $1.82 million.

To no one's surprise, cyberinsurers have increased premiums – and their requirements to qualify for a policy are much stricter.

Recently, policy exclusions of coverage have grown, and include failure to maintain cybersecurity standards, payment card industry fines and assessments, prior acts, acts of war and more. The failure to maintain cybersecurity standards exclusion is particularly deadly – as we have had to explain many times to clients who refused to implement multifactor authentication (MFA) because it was "inconvenient." Fortunately, most law firms now accept, however reluctantly, the need for MFA.

Insurance requirements continue to become more stringent. You may have to institute regular cybersecurity awareness training or abide by a specific timeline for applying security patches. All law firms must be sure that they adhere to all requirements or risk falling under an exclusion provision. Thinking your firm is covered when it may not be is a recurring nightmare these days.

Prior Acts Can Be a Major Headache

The average time to detect and contain a data breach is 277 days according to IBM Security's *Cost of a Data Breach Report 2023*. Why is that so important? Your policy may carry a "prior acts exclusion" for things that took place before the retroactive date or the first date of a policy.

What can you do? If you are going to a new insurance company, you can probably purchase an extended discovery period that will cover claims arising from a time previous to the start of your new policy. While it will cost you something, it may be worthwhile.

What About Acts of War?

It's thorny. There are LOTS of nation-state attacks on law firms. But is that an act of war? Recently a New Jersey court determined that an insurer couldn't claim an acts of war exclusion because the policy language applied to traditional forms of warfare and not to cyberattacks. That 2022 decision was affirmed by a New Jersey appellate court in 2023.

What do we think will happen next? Likely, insurers will change the exclusion to include non-traditional forms of warfare. From the insurer's point of view, that is the only logical alternative – and that exclusion has already been instituted by some insurers who foresaw this problem within the last couple of years.

Final Words

We couldn't top the wisdom of ChatGPT: "Cyberinsurance for attorneys is like an umbrella that leaks a bit in a storm – nobody really likes carrying it around, but getting caught without any umbrella at all is even worse." Absolutely true!

Sharon D. Nelson *is a practicing attorney and the president of 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 vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com*