Cyberinsurance Bedevils Law Firms

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

Procuring Cyberinsurance: An Annual Nightmare

When lawyers receive their annual cyberinsurance policy for review, they become apoplectic. Typically, cyberinsurance costs more each year and offers less coverage. To add fuel to the fire, lawyers are faced with a lengthy form to fill out detailing many aspects of their cybersecurity. The questions, for many lawyers, are incomprehensible. Forget about accurate answers – they need to bring in their IT professionals to help, another cost if they rely on IT help outside of the firm. The problem is further complicated if the IT professionals do not carry a cybersecurity certification.

Worse yet, if a firm investigates getting a cyberinsurance policy from multiple cyberinsurers, the first thing they'll discover is the truth of a popular saying. "If you've seen one cyberinsurance policy, you've seen one cyberinsurance policy." The variations between cyberinsurance policies are truly remarkable – and utterly confusing for lawyers trying to obtain coverage.

Cyberinsurance Policies and Law Firm Cybersecurity

While most lawyers now recognize the need for a cyberinsurance policy, they frequently find themselves balancing the risk of a breach – and the financial consequences – against the cost of cybersecurity measures required by the cyberinsurance policy.

Those measures are constantly evolving – we remember well how our clients balked at adopting multi-factor authentication (MFA) – until they realized they could no longer get cyberinsurance without adopting MFA. This was certainly a needed requirement, but the resistance in the early days was fierce.

Clearly, big firms weren't going to have problems with funding upgraded cybersecurity, but it was rough on smaller firms trying to find the funds to meet the demands of the cyberinsurance companies.

The Magic of a Good Broker

Make no mistake about it. The secret to getting a good deal is to have a good broker, someone who works with lots of cyberinsurance companies and knows how to match you with the cyberinsurance company with the right coverage at a price you can afford.

We came by that advice honestly, as were beyond frustrated by the cost of our cyberinsurance and the restricted coverage. A friend recommended us to a broker and,

mercy of mercies, we found good coverage at a price we could afford. The added bonus was policy language you could understand.

The Rise of Privacy Laws

We are now up to 18 states with privacy laws (some not yet in effect)– with more to come. This has been a game-changer for cyberinsurance, as law firms will be accountable for the data they collect and what they do with it.

A veritable tide of privacy laws are expected to pass in the next year or two, so attorneys need to be prepared, as cyberinsurance companies will surely raise prices to cover violations of privacy laws.

It's Not Just About Data Breaches

Attorneys need to get themselves out of the mindset that they are only protecting against data breaches. One common example is wire fraud – no breach there, just a wily criminal who manages to get someone at the law firm to wire them money. These days, with deepfakes on the rise, the poor person who is attacked may actually "see" someone they know giving the wiring instructions.

What other expenses are there that you need covered by your policy? You may need a data breach and/or privacy law lawyer, digital forensics assistance, and a public relations firm. Does the policy require you to use resources provided by the cyberinsurance company? That seems a bit of a sticky wicket to us. How much can you trust someone who is beholden to the cyberinsurance company?

What's Excluded from Your Policy?

What's excluded is important. Probably the exclusion most feared by law firms is the exclusion of coverage for state-sponsored attacks. It isn't always easy to determine whether or not an attack is state-sponsored.

Your coverage may have a retroactive date, so that the insurer has no liability for acts that occurred prior to a certain date, often the date of inception of the policy. So if you had a data breach before the inception of the policy which came to light once the policy was in place, you are out of luck.

If you failed to maintain required cybersecurity measures, you may find coverage refused.

And for heaven's sake, don't forget to timely notify the insurance company – and yes, we've seen coverage denied for that!

Cyberinsurance Claims Are Escalating

According to cyberinsurance broker Marsh, it received more than 1800 cyberinsurance claims in 2023, bashing all previous records. Why? According to Marsh, the sophistication

of attacks is rising, privacy claims increased, and more businesses have cyberinsurance, which raised the number of claims.

Final Thoughts: AI: Revolutionizing Cyberinsurance

Artificial Intelligence and Large Language Models are everywhere, so why not as part of cyberinsurance? More and more cyberinsurance companies are focused on reducing the probability of a breach, constantly evolving cybersecurity strategies. Risk assessments are now being based on AI-driven insights providing real-time risk assessments.

As a nice thought for those who have filed claims, AI is now cutting claim processing times by over 80%. Most impressive and very welcome!

Sharon D. Nelson *is an 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 Chief Executive Officer at 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*.