Cyberinsurance: More Expensive, Less Coverage

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

Cyberinsurance Sticker Shock

We've been watching cyberinsurance get more and more expensive over the years. Perhaps in the wake of the extraordinary number of data breaches in 2023 (both small and large organizations), it is no wonder that a recent survey showed that respondents report an increase in insurance rates of 50-100% upon initial application or renewal.

Ouch. You must also prepare yourself for an ordeal of six months or more to obtain or renew cyberinsurance.

The August 2023 report from Delinea caused a lot of eyebrows to go up. Almost 80% of survey respondents have used their cyber insurance policy. Half of them needed to use it multiple times. That's more than a little blip!

Cyberinsurers Slash Coverage

Slashing coverage was rare a few years ago, but now you need to read the fine print carefully, something which many lawyers are not doing. What could void your coverage?

- Lack of adequate security protocols (43%)
- Human error (38%)
- Acts of war (33%) – read carefully so you'll know if "state sponsored attacks" (very hard to prove sometimes!) are covered
- Not following the required compliance procedures (33%)

We would add a requirement for annual cybersecurity awareness training for law firm employees – and attendance should be mandatory and documented. In fact, some carriers specifically ask about (or demand) employee training efforts.

And, of course, if you lie on the application, denial of coverage is likely. Sadly, we have seen applicants check a box which they know darn well shouldn't be checked.

Security Solutions are Required

Most organizations (96%), including law firms, have to buy at least one security solution before their application is approved. 51% of respondents to the survey indicated that Identity and Access Management and Privileged Access Management (49%) are required. Why? Because most attacks involve stolen credentials.

Fundamentally, the insurance companies are enforcing good cybersecurity, often compelling applicants to budget for extensive cybersecurity measures. Since we often help law firms understand what cyberinsurance companies are requiring, we can tell you that they are

dumbfounded by the changes required, not only the higher level of security, but the price tag that goes with it.

Trying to explain some of the measures above along with anti-malware software, encryption, firewall and intrusion detection, the importance of patching quickly, vulnerability management, password management etc. is a challenging task. Cyberinsurance carriers will want you to implement a few technology solutions such as multi-factor authentication (MFA) and endpoint detection and response (EDR). Don't worry. There are several solutions that vary in cost from free to very affordable even for a solo attorney.

Even policy claim procedures have gotten tougher – fail to follow the claim procedures scrupulously and you may find your claim disapproved.

What's the Bottom Line on Cyberinsurance?

Very likely, it will be harder to get cyberinsurance and it is likely to have less coverage. Many insurance companies are still figuring cybersecurity out. A lot of them have found that their risk assessment models were not correct. And it is certainly true that insurance companies are not in the business to lose money.

As their understanding deepens, requirements are likely to get tougher to meet, especially for smaller law firms.

A shoutout to Marsh LLC is warranted for developing its Cyber Pathway insurance program. The Cyber Pathway permits Marsh clients that had been found uninsurable for cyber risks to procure coverage as they followed the Pathway to improved cybersecurity. There are a lot of specifics in the Pathway, which makes it easier to follow and to obtain coverage.

Final Words

One of the things we have learned is this: It is all about the broker. Most brokers are not cyberinsurance specialists – and that's exactly what you need. By using a knowledgeable broker, we ended up paying less and getting more coverage – the precise result we are all looking for!

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*