Pay More, Get Less: Cyberinsurance Now a Nightmare for Law Firms

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

Yes, the Sky is Falling

Ever since cyberinsurance came on the scene, law firms have been fretful about the rising costs. Through most of 2021, we were seeing price increases of 30-40%. But according to global insurance company Marsh, the price of cyberinsurance in the U.S. grew by a stunning 130% in the 4th quarter of 2021. Commercial insurance, by contrast, rose only 13% in the final quarter of 2021. The cyberinsurance carriers will say that the market was undervalued to begin with, and the increases are value adjustment corrections.

Insurance companies often have reinsurance policies they buy to protect themselves from steep claims – and the price of reinsurance has increased as well, further spooking insurers, some of whom have withdrawn from offering commercial insurance, leaving less capacity in the marketplace.

Basically, we've been watching a train wreck in cyberinsurance, with no end in sight.

Is This All About Ransomware?

Pretty much. London based Beazley has said that prices will increase as claims, especially ransomware claims, increase. The financial impact has been so severe that some insurance companies have decided simply to drop cyberinsurance as an offering.

Others have taken Draconian measures.

The Register reported on November 30, 2021, that Lloyd's of London may no longer extend insurance coverage to companies affected by acts of war.

The insurer's "Cyber War and Cyber Operation Exclusion Clauses" include an alarming line suggesting policies should not cover "retaliatory cyber operations between any specified states" or cyber-attacks that have "a major detrimental impact on… the functioning of a state."

Lloyds published four different clauses as suggestions for insurers in Lloyd's-underwritten policies. It seems likely that some insurers will adopt some of the clauses.

According to The Register, "The policy clauses also raise the idea of insurance companies attributing cyber-attacks to nation states in the absence of governments carrying out attribution for specific incidents, an idea that seems extremely unlikely to survive contact with reality."

Truer words were never spoken. This would be, as our British friends would say, a bloody mess. Nation state attacks are common – and the line between a Russian state attack and an attack by ransomware gangs harbored by Russia could get very blurry.

Increased Premiums, Increased Deductibles and Decreased Coverage

Read the header above again because that's what you'll be facing when you go to renew your cyberinsurance coverage. Take a close look at the exclusions, because they may have expanded significantly so paying a hefty increase in premiums may be buying much less than you think.

Exclusion clauses now often include acts of war, failure to maintain standards (more on that later), payment card industry (PCI) fines and assessments and prior acts. Prior acts exclusions prevent a claim for activity that took place before the retroactive date or the first date of a policy. This exclusion is important because data breaches are often not detected until long after they occur.

A New Jersey Superior Court judge recently ruled on an acts of war exclusion lawsuit. The case dealt with the 2017 Russian cyberattack on Ukraine, known as the NotPetya attack, which impacted U.S. businesses including pharmaceutical giant Merck & Co.

Merck claimed it incurred $1.4 billion in damages and filed a claim with its insurer. The insurer denied coverage based on the acts of war exclusion. Merck sued. In January 2022, the judge ruled that the insurer can't claim the act of war exclusion because the language in the policy applied to traditional forms of warfare, not cyberattacks. The insurer was required to pay the claim to Merck.

You can be sure insurers are altering that kind of exclusion as we write this article.

The Failure to Maintain Security Standards: An Escape Route for Insurers

A typical day in the office includes a call from a worried lawyer at a law firm telling us the firm has received a 20 page cybersecurity application form with questions no one really understands. Managing partners have the dismal feeling that they can't truthfully answer the questions the way the insurance company wants them to.

No question about it – the insurers now have a long list of questions designed to help them deny claims if you don't keep up with required security measures. The language of a "failure to maintain standards" exclusion varies widely.

You should ask an insurer to remove any ambiguous language in a cyber policy to ensure that the standards are clear. Does the insurer require use of basic controls like encryption or multifactor authentication? Do they specify the MFA methods that are acceptable or is the MFA question silent on the type, therefore allowing you to implement SMS text messages which are subject to SIM swapping attacks? Are there specific regulatory obligations required for compliance? Does the insurer require periodic training, testing, or upgrades in technology during the policy period?

How much room is there for negotiation? Not much, in our experience. Presumably, the insurance companies have qualified cybersecurity experts helping them design the required security standards, but we've seen many standards which do NOT indicate a deep understanding of cybersecurity or reasonable ways to reduce risk.

Nonetheless, it is almost a take it or leave it proposition from the insurer's point of view. Our own prominent insurance company wrote these words:

"*If we do not hear back from you by 02/24/2022 or unacceptable answers are received to these questions, we will need to send notice of non-renewal for the Professional/Cyber policy."*

Charming after decades of loyalty to an insurer without a single cyber claim, isn't it? And this scenario is being repeated at law firms of all sizes.

How Does a Law Firm Protect Itself?

It remains to be seen whether cyberinsurance companies will mandate so many exclusions, co-pays and deductibles that their policies aren't worth purchasing. As it is, 64% of small and medium-sized businesses do not have cyberinsurance coverage, according to an August 2021 report by Statista.

Too many law firms are now buying insurance and thinking, "We are good to go now." That's a mistake. We need to change that mindset. Cyberinsurance is fine if you can find good insurance at a reasonable price but proactive security is critical to law firms – and often under-emphasized.

Get a security assessment from a reputable cybersecurity firm – you should be able to get a reasonable flat fee that includes a detailed report of critical vulnerabilities to be addressed immediately, medium vulnerabilities that you can take a little time to budget for, and more minor vulnerabilities that you can deal with later.

If you been avoiding MFA, stop avoiding it. It may be a minor nuisance, but it is usually free – and very effective. If you don't have technology to monitor and respond to cyberattacks, you're asking to be breached. If you're not yet implementing Zero Trust Architecture, don't wait another day to embark on that inevitable journey.

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.