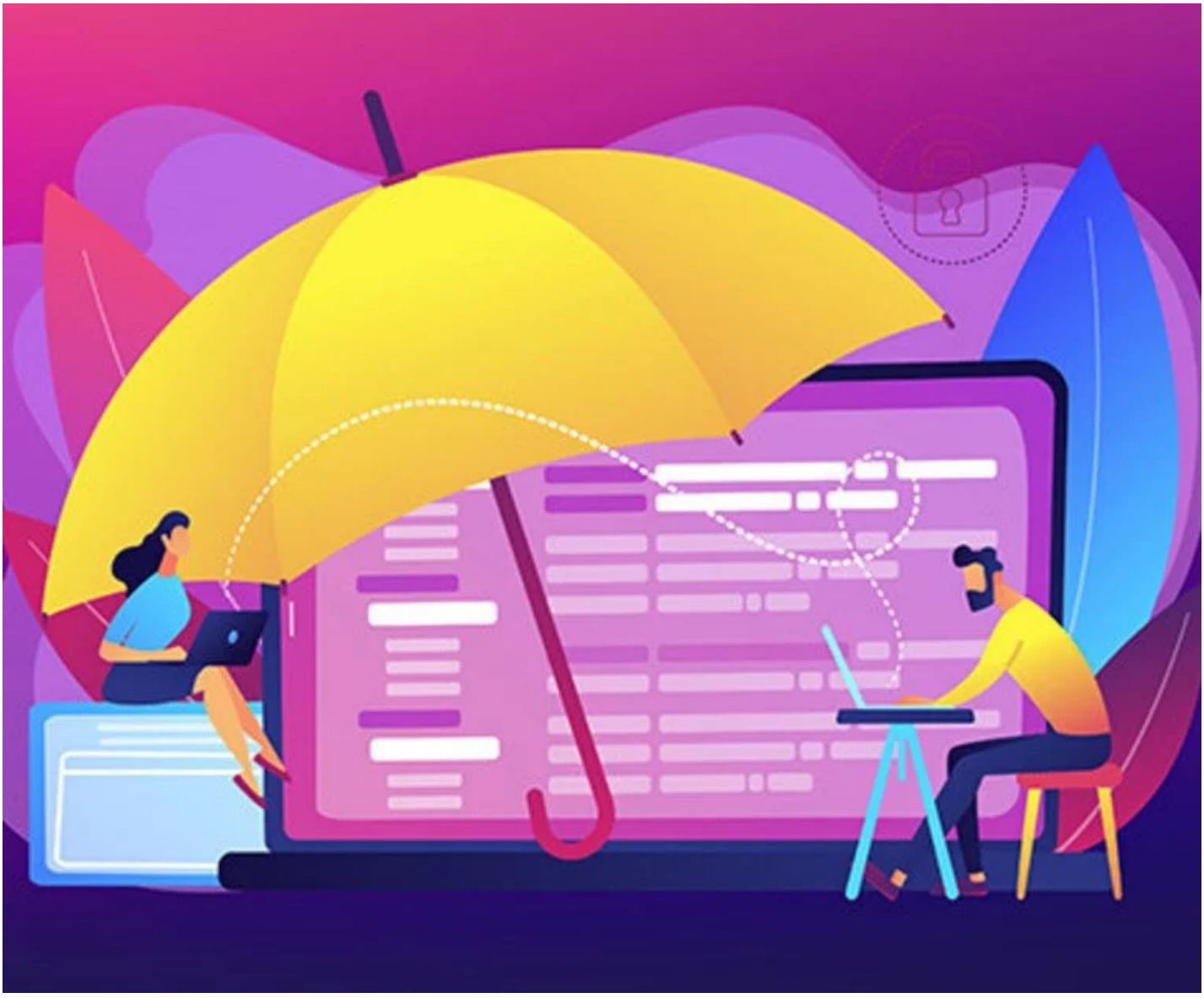
Legaltech news

As Cyber Insurance Evolves, Firms Face More Requirements, Rising Costs

With some cyber insurance companies closing up shop, premiums are likely to spike, while obtaining coverage will likely require many firms to step up their own cybersecurity defenses.

By Isha Marathe | June 22, 2022



Few other threats have seen the level of incline as cyberattacks. Of course, for businesses and firms, the one saving grace has generally been cyber insurance, providing them with a level of financial security from a usually invisible enemy.

However, cybersecurity experts reading the tea leaves warn that in the near future, cyber insurance won't be the padding it once was.

As all U.S. verticals from infrastructure to legal brace themselves for a uptick of cyberattacks from Russia (https://www.law.com/legaltechnews/2022/04/29/ukraine-russia-conflict-prep-4-ways-firms-should-strengthen-their-cybersecurity-efforts/), some cyber insurers are jumping ship, unable to accommodate the financial losses. In turn, premiums are shooting up and coverage is becoming more selective.

While the biggest brunt of the cyber insurance landscape becoming more expensive and concentrated will be faced by smaller firms and solo attorneys, experts say one thing is clear: Law firms of all sizes will have to meet insurers halfway when it comes to securing their cyber defenses.

Mark Sangster, chief of strategy at security software company Adlumin, said the days of firms' "fatalistic philosophy" of blindly relying on cyber insurance are numbered.

"Cyber insurance is not a 'get out of jail free card' anymore," Sangster said. "The days of saying, 'We have insurance, so if we get shut down by ransomware, it's no big deal, we can just make a claim and be whole again' are gone. Because of the last couple years, the majority of policies that have claims made against them lose money for the underwriters. That's going to be the economic model insurance companies are going to live with from now on."

To be sure, Sangster doesn't necessarily see this as a bad thing, but instead as a move that will force firms "to put skin in the game." Firms will now have to be more proactive about regular awareness training, ensuring safe VPN connections, multifactor authentication and "at least minimum security standards" so, if there is a breach, "they can demonstrate [to insurers] that [they] were prepared to do incident response."

Of course, focusing only on more cybersecurity preparedness won't help. With U.S. cyber insurance costs reaching nearly $5 billion in 2021 (https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html), according to Munich Re's 2022 Cyber Risk and Insurance Survey, and a growing number of ransomware attacks last year, underwriters will have to put far more energy into figuring out just what their insurance covers (https://www.law.com/insurance-coverage-law-center/2022/06/15/with-the-rise-in-ransomware-will-your-insurance-cover/) and what it will cover in the coming year.

"This isn't like renewing your auto insurance where it just auto-renews," Sangster added. "It's a lot more complex. You can't just put on blindfolds and drive because you have health insurance or auto insurance. It's the same for cyber insurance."

Indeed, John Simek, vice president of security support company Sensei Enterprises, noted that cyber insurance disclaimers are changing each year. Disclaimers that once consisted of "basics" like "multifactor authentication" are getting more in the weeds.

"We are starting to see more specific requests than before. One is about remote access technology, the other is endpoint detection and response [EDR] and they ask about the capabilities of each solution because not all EDR is created equal," Simek said. "They don't just ask you about the actual company or software you're using, they want to know the capabilities."

Simek said the growing application questions don't just end with the company seeking insurance, but spill into what vendors the company is using and their cybersecurity protocols as well.

"The application questions are not really requests, they are demands," said Sensei president Sharon Nelson. "If you answer no to a question, they are going to tell you they are not going to insure you until you do it."

To make matters more complicated, Nelson and Simek said they have seen a "significant" number of insurance companies pack up shop in the last few years, further thinning the pool and pushing premiums higher.

"It's especially the solo and small firms that feel like they are being priced out of cyber insurance because it's so expensive," Nelson said. "Insurance companies are in the business of making a little bit [of money], they are certainly not in the business of losing. Cyber insurance is moving very rapidly in all kinds of directions. There are less choices now. Not the majority, but many carriers have just said, 'To hell with it. We are not doing it anymore.'"

To be sure, continuously rising premiums alongside a spike in cyber threats is not the most sustainable scenario for any industry. Tom Bossert, president of Trinity Cyber and former Homeland Security adviser, believes the future might see more of an intersection between property and casualty insurance and cyber insurance.

"If by a cyber means a hacker or a nation state breaks all of your computers, now it turns them all into paperweights and the cost that a large corporation would incur if they had to replace all their corporate hardware, it would be a large property claim," Bossert said. "I think the future world for cyber insurance and for property casualty insurers has to do with the intentions of our cyber adversaries."

Essentially, if attacks go beyond "stealing credit card information" and are intent on causing damage, then many cyber insurance claims will actually spill into property casualty claims, he noted.
