More law firms are buying cyber insurance, but not all

*by **Gregg Wirth***

Before the global pandemic, cyber-threats were escalating and the next major data breach seemed to be just a headline away. Now, as the cyber-criminals become emboldened as countries and industries scramble to return to some semblance of a new normal, these threats are even more dire.

As a result, **law firm** leaders are facing considerable pressure to protect their data and that of their clients. But what comprises a reasonable investment in that area, and what are the best ways to prioritize data security?

Not surprisingly, the idea of **cyber insurance** — policies that will help mitigate the financial damage done by cyber-incidents — continues to gain considerable ground, especially among law firms. Now, with more pressures mounting on business, some worry that law firms — many of which had been resistant to the idea previously — may forget it altogether amid competing challenges during the current crisis.

Tom Ricketts, Senior VP and Executive Director at **global insurance broker** and **risk advisor** Aon, says that just six years ago when he joined the firm, only about a half dozen of the firm's 300 law firm clients were buying cyber insurance. "Now, we estimate the uptake is about 60% of our law firm clients and maybe another 10% to 20% or so buying it elsewhere," Ricketts says. "But many large law firms are not buying cyber insurance at all, despite the ever-increasing frequency and severity of cyber-incidents."

Ricketts is the Cyber Insurance Practice Leader with Aon Risk Services in New York, working with the firm's Professional Services Group that serves law firms, accounting firms and consulting firms. Ricketts estimates he spends 90% of his time working with law firms.

While it's still too early to comment about the impact of the pandemic on cyber insurance buying, Ricketts says there is no question that clients understand the change in the threat environment that has occurred. "We have had many discussions with clients about the implications and the details of coverage as it applies to a remote workforce, he adds.

Cyber-incident costs are not incidental

"Cyber insurance today is a really interesting environment," Ricketts says. "There is no getting around the evidence that law firms are being increasingly targeted, and the perception is that they are an easy target."

While admitting that he has self-serving reasons to wish for a 100% buy-in of cyber insurance, Ricketts explains that the main reason there is still a relatively low uptake of cyber insurance among law firms is because of economics. "There is always this perception that cyber insurance is expensive, that it seems like a big spend," he says. Associated with that, he adds, is the belief among some law firms that their only real exposure is client data, so if they do get hacked and the data stolen turns out to be client data – often perceived by hackers as the real treasure within law firms – the firm's professional malpractice insurance is all the cover they need.

However, Ricketts advises, it is a misconception that professional liability insurance will cover firms for everything related to a data breach, and he likens it to the all-too-frequent expectation that insurance will cover everything. For example, news reports following the floods in New York and New Jersey after Hurricane Sandy showed that many homeowners assumed that their household policy covered them for any damage to their home, only to find that flood damage was excluded. “Lawyer’s professional liability policies are very broad, but like homeowner’s insurance there are certain risks, such as loss of revenue, that they do not cover,” Ricketts says.

“Some of these firms that have had cyber-incidents have suffered a major loss of revenue, or they’ve incurred significant expenses to remediate their systems,” Ricketts explains. “And this is really where the value of cyber insurance comes into play because those expenses can be enormous.”

Aon has seen examples of law firms that have incurred costs in the millions of dollars within weeks of the start of a cyber-attack, Ricketts says, adding that some firms have racked up bills around $2 million-plus, paying for forensic investigators, security companies, consultants and breach counsel (an external law firm to help them manage the breach). “There’s a lot of expense that amasses very quickly, and these expenses are very unlikely to be covered by a professional malpractice insurance.”

Aon’s numbers reflect the growing importance of cyber insurance coverage. Even as the percentage of its clients buying cyber insurance has swelled over the last five years and those firms are purchasing in the aggregate $2.5 billion of coverage, the cost of this insurance has been decreasing as a proportion of the firm’s revenue. “So, it’s a good time to be buying cyber,” Ricketts quips.

Indeed, Aon’s data shows that an average law firm’s limit purchased correlates quite closely to the firm’s annual revenue, in a relatively narrow band of 1% to 4%. Interestingly, there seems to be no correlation between the limit purchased and a firm’s attorney count, which Ricketts suggests might be more reflective of the exposure than revenue; according to one study, over 80% of cyber-incidents start with a human element failure.

On the other hand, the average law firm’s spend on its cyber insurance premium correlates very closely to both the firm’s annual revenue and its attorney count, indicating at least that the *purchase* decisions around cyber insurance are driven by economics – specifically, the interplay between the size of the firm and the premium cost, he explains.

As a benefit for firms considering purchasing cyber insurance, the cost of a policy has fallen quite dramatically, he says. Five years ago, a $10 million policy would have cost $250,000 or more; now, you can expect to pay $120,000 or less depending on the size of the firm.

Why the decrease? The insurance industry itself is starting to solidify around the idea of cyber insurance. “The insurance industry at the moment sees cyber insurance as profitable,” Ricketts explained, adding that insurers are still building their book of business with the product. “Of course, the frequency and severity of incidents are also going up, so that profitability is starting to decline but not to a point where it’s underwater.”

Balancing cost & need

So, how much cyber insurance coverage will you need to bail your firm out of a catastrophic incident – and truthfully, aren’t they all catastrophic, especially if you’re on the receiving end? Ricketts says he’s seen published estimates that peg the financial damage of a cyber-incident at between $3.5 and $4 million, but he says there are qualifications to that.

“First, that’s a global number, so you’re looking in countries where the costs of remediating the loss are very, very low, compared to the US,” he says, adding that secondly, the poles of the losses are quite different, with the vast majority of incidents costing maybe less than $1 million, but several high-profile losses costing up to $40 million. “So, that average of $3.5 million – I doubt if anyone saw that number.”

In the US, not surprisingly, the average cost for a cyber loss is much higher, an estimated $11.5 million, Ricketts says. But this too can be similarly misleading because while the *average* is $11.5 million, the *median* is around $1 million, he explains. “That likely means your loss is either going to be $1 million or $20 million, or $50 million – so, having $11 million in coverage is not necessarily where you want to be.”

Ricketts says it’s also worth mentioning that despite the technical complexity and high-pressure panic that a cyber-incident might involve, cyber insurance does pay out when needed. Indeed, cyber insurance has a higher payout rate than that of any other type of insurance, according to the Association of British Insurers, which cited that out of 207 recent claims, 99% were paid.

Clients want coverage

Another factor impacting how law firms view cyber insurance is their clients’ desire that their outside counsel be covered in cases of cyberattacks. In fact, in its recent guidelines for external counsel, the Association of Corporate Counsel cited the need for external counsel to have a minimum of $10 million of cyber insurance coverage.

“Clients of law firms are getting more demanding and more granular about what they expect their law firms to have as a cyber insurance program, and that is unquestionably driving a lot of purchases,” Ricketts notes, adding that Aon and other insurers saw an immediate effect within weeks of those guidelines being published and that has definitely continued as a trend over time.

“Cyber insurance is a maturing product,” Ricketts says. “There’s no question that people are beginning to understand and appreciate its value. Every one of our law firm clients that has had a cyber-claim has immediately bought more coverage at the next renewal.”

And, as the legal industry navigates the difficult terrain of the pandemic crisis, and tries to envision what the next new normal might look like, cyber-insurance will likely play an increasingly crucial part.

This article originally appeared in the Spring 2020 issue of Forum magazine. It was also published on June 3, 2020 on Thomson Reuters’ Legal Executive Institute blog: *More law firms are buying cyber insurance, but not all*

If you’d like to discuss any of the issues raised in this article, please contact **Tom Ricketts**.