Cyberinsurance: Necessary, Expensive and Confusing as Hell

by Sharon D. Nelson, Esq. and John W. Simek

Setting the stage

The title of this article was also the tile of a session presented at ABA TECHSHOW this year. And each part of the title is true. It is absolutely necessary to have cyberinsurance in order to manage your risk. No amount of technology, policies or training can guarantee that you will not be breached. Expensive? Oh yes. Get ready for sticker shock when you purchase cyberinsurance. Because we teach CLEs on cyberinsurance, we can tell you with some assurance that lawyers are very confused about what specific insurance they need. Insurance companies are not very helpful– the various policies offered across the industry are not at all standardized – and of course they are written in complicated language which often obfuscates their meaning.

Where are we today?

Not in a great place. According to a 2017 survey by the data analytics firm FICO, half of U.S. business have no cyberinsurance, 27% have no plans to buy coverage and only 16% report having a policy that covers all cyber risks. There is a certain justified cynicism about cyberinsurance. The news is rife with companies who had cyberinsurance, but found – after being breached – that a substantial portion of their damages were not covered.

A 2017 report by Deloitte called "Demystifying Cyber Insurance Coverage" called the market "promising" but "problematic" for the insurance companies as well as customers. We don't have a lot of data going back in time to help us construct reliable predictive models. With threats evolving daily and many different kinds of damages possibly occurring, perhaps over a broad swath of insurance company customers, insurers are "flying blind" – something you can see for yourself when you look at widely varying prices for widely varying coverage. As a result, many insurers are focused on PII (personally identifiable information) coverage which may or may not be the primary need of an organization. Chubb Group, a well-known and early entrant into the cybersecurity market, paid some of the losses for P.F. Chang's point-of-sale data breach but it did not cover the required $1.9 million Payment Card Industry Data Security Standard assessment. If you don't even know what that means (and many lawyer do not), take a deep breath and do a search on PCI-DSS fines . . .

And after all this time, many law firms and other entities mistakenly believe that their general liability or business interruption policies fully cover data breaches. Some of them have learned the hard way how very wrong they were.

Given the fact that law firms are generally not models of strong cybersecurity practices, it would be prudent of law firms to up their game, especially since both clients – and potential insurers – are asking hard questions about firms' security. In 2017, legal technology firm LogicForce gave the legal industry only a 42% rating on its cybersecurity health. The score was based on twelve factors, weighted differently, including information on information security executives, polices, multifactor authentication, cyber training (we have seen a big uptick there), cyberinsurance, penetration testing, vulnerability testing, third-party risk assessments, information governance, cyber investment, full disk encryption, and data loss prevention technology and software.

Apples to apples comparisons?

Fuggedaboutit. The best you can probably do is to consult a trusted insurance advisor who is accustomed to dealing with cybersecurity policies. Once you get over the aforementioned sticker shock for the costs of the policy and absorb the grim reality of the high deductibles, you've got to get into the nitty gritty of a subject that is very hard to understand if you are not in the insurance business with a keen understanding of cybersecurity.

In many cases when lawyers ask where to get impartial advice, we are apt to recommend that lawyers ask their colleagues for references – not so much here because, unless your colleagues have suffered damages from a cyber attack or breach, they really don't know how good their policies are.

Most lawyers have professional liability insurance, which will undoubtedly get you some cyberinsurance coverage since you are holding data because you are rendering legal services. However, more than 50% of the cost of a data breach may come from digital forensics and the data breach lawyer you hire – which are not covered by the LPL (Lawyers' Professional Liability) policy. Other costs which are likely not covered include public relations coverage, data breach law compliance/notification costs, regulatory investigations costs, including subsequent fines and penalties.

What will cyber insurers likely need to know before giving you a quote?

Clearly, the information sought will vary from insurer to insurer, but here is a likely list of questions they might ask and things they will require:

1. Have you had an independent 3rd party cybersecurity audit? And yep, they'll want the results and an accounting of any remediation that was performed.
2. Do you have e-mail encryption available for use? Is it used?
3. Do you employ full disk encryption?
4. A description of how your backup is engineered – to make sure, if you contract ransomware, that you have a reliable backup that you can restore your data from.
5. Do you train your employees in cybersecurity and how often you train?
6. Your security-related polices.
7. What kind of enterprise level security software and hardware are deployed, including firewalls, data loss prevention, incident detection software, etc.?
8. Have you ever experienced a data breach or other major cybersecurity incident? Yes, they will want details, including how long it took to discover any breaches.
9. A description of the physical security of your premises.
10. Do you comply with any national/international cybersecurity standards?
11. Have you ever made an insurance claim involving cybersecurity? Details will be required.
12. Has any other insurer canceled your cybersecurity policy or refused to renew one?
13. Mobile device security in place, which can cover a lot, but they will certainly want to know if you can remotely wipe lost or stolen devices.
14. Details of vendor management for those who have any degree of network access or who hold your data by design – are audits of those vendors required?
15. When employees are processed out of your firm, what measures are taken to secure your data?
16. Do you do background checks on new employees? Are they trained in security policies?
17. Awareness of facts which might give rise to a possible claim at the time the application is filled out.

18. The amount of your annual cybersecurity budget (particularly true for larger firms).
19. Are you following general best practices regarding passwords, access control, patching and upgrading outdated software which is not receiving security patches?
20. A description of the kind of data you hold (health data, credit card data, banking records – any sort of protected data).
21. Financial data about your firm, including assets, revenues, number of employees and any proposed merger or acquisitions.
22. Is logging enabled? What is the retention period of log files?

The list of possible insurer questions can seem daunting, especially if you become aware that your truthful answers (and failure to be truthful may invalidate coverage) will not please the prospective insurer.

What should you be asking a prospective insurance company?

This can be a hard question, but we have found it useful to set forth specific scenarios with specific damages and ask the insurance agent to show us what language covers what damages. For instance, virtually all insurance policies cover actual loss or damage to your computers, but not the loss of the data. Can you sometimes negotiate the coverage itself? Absolutely. Of course, that may come with a price tag. Taken together, the premium, the deductible and the coverage should give you a fairly clear idea of how well you are managing the risks you cannot wholly protect against – and the price for doing so. And if you don't like one proposal, well, there are now more than 60 carriers offering cyberinsurance, so you certainly have alternatives.

If your data is in the cloud or otherwise held by third parties, you are certainly going to need third party coverage. If your firm is active with social media coverage, you may need media liability coverage. And when regulatory fines loom, and they often do these days, you certainly want coverage for regulatory fines.

Ask your insurer as many questions as you can think of, but here are a few starters.

1. Is the coverage retroactive? How far back, if so?
2. Does the insurer believe your limits of coverage are adequate for your needs, especially given the nature of the data you hold and the size of your firm?
3. Does the policy cover both the loss and the compromise of data (e.g., make sure data encrypted by ransomware is covered)
4. Is there a discount if you have a 3rd party independent audit and remediate any critical vulnerabilities found by the audit?
5. Are you covered if a vendor holding your data suffers a breach?
6. For an additional premium, does the insurer offer a subrogation waiver? We know some of you are asking "What's this?" Google it for the full explanation and why such a waiver may be desirable. Where is cyberinsurance going?

Final Thoughts

Fitch Ratings said the industry grew by 35% in 2016. Allied Market Research predicted that the global market may reach $14 billion (now that's a big number) by 2022. But if you want a queasy stomach as you fork over huge premiums, consider this quote from Tim Francis, a vice president and enterprises lead for cyberinsurance at Travelers: "There's so much new coverage out there that hasn't been tested .

. . One day there will be certain claims and we'll figure if the words we used to convey coverage actually say what we thought they meant, which is often up to a lot of lawyers." Not very reassuring, is it? The world of cyberinsurance is evolving – think how little we have by way of precedents. Combine that with the rapid changes in attack surfaces, cyber weapons and tactics, etc. and it is a bit unsettling. As we have now reached the point where many firms have been breached – and will be breached again - the one thing we can tell you for sure is that cyberinsurance is essential risk management for law firms.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com