The Computer & Internet Lawyer

Volume 33 ▲ Number 12 ▲ DECEMBER 2016

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

A New Dawn for Law Firm Cyberinsurance: "We Don't Insure Stupid"

By Sharon D. Nelson and John W. Simek

It would be too strong to say "forget everything you knew before" about cyberinsurance, but there have been such major developments in the last year that a strong cup of coffee might be helpful while you carefully read this article. A new dawn has indeed broken and law firms have a lot of catching up to do.

How Good Is Your Cyberinsurance? Do You Know If You Have It?

In the American Bar Association's (ABA) 2015 Legal Technology Resource Center Survey, only 11 percent of respondents knew their firm had cyberinsurance. That's alarming when the same survey showed a marked increase in data breaches and security incidents. The survey showed that many lawyers didn't know whether their law firms had cyberinsurance—in fact, in firms of more than 100 lawyers, 80 percent didn't know if the law firm carried such insurance. Now that the ABA Model Rules of Professional Conduct have required more technological competence of lawyers (Rules 1.1 and 1.6, thus far adopted by 15 states, and that number expected to grow), it may be an ethical violation if you don't inform yourself about the state of your firm's information security and, of course, one way you protect your clients is by managing risk through cyberinsurance.

Lawyers often insist that their comprehensive general liability (CGL) policy will protect them. It almost never does. Almost all insurers have now riddled the CGL with exclusions to push clients into new, specialized cybersecurity insurance policies or riders. Cyberinsurance is its own beast, and a law firm without it in our breach-laden world is very foolish.

The Rapid Evolution of Cybersecurity Policies

Cybersecurity insurance policies, first introduced in the 1990s, are now the fastest growing segment of the insurance industry. As of 2015, according to a report from insurer Allianz Global Corporate and Specialty (AGCS), the cyberinsurance market is estimated to be worth around $2 billion in premiums, with US businesses accounting for about 90 percent of the market. Although fewer than 10 percent of companies in the United States

Sharon D. Nelson is president of Sensei Enterprises, Inc., a legal technology, information security, and digital forensics firm based in Fairfax, VA. **John W. Simek** is vice president of Sensei Enterprises, Inc.

Wolters Kluwer

purchase cyberinsurance today, the market is expected to grow by double-digit figures from year to year and could reach more than $20 billion in the next decade. And no wonder—a recent study by the Ponemon Institute estimates that more than one billion records of personally identifiable information have been stolen worldwide to date.

The Myth That "It Can't Happen Here" Has Vanished

It is now widely accepted that most large law firms have been breached, many more than once. Put another way, there are two kinds of law firms—those that have been breached and those that will be breached. Very simply, data that has value (and is usually sold on the Dark Web) is a magnet for the bad guys.

A recent study by the Ponemon Institute estimates that more than one billion records of personally identifiable information have been stolen worldwide to date.

Why is cyberinsurance such an important part of information security? The plain truth is that information security has no silver bullet. You can never secure your data 100 percent of the time. A determined and sophisticated hacker can overcome your technological defenses.

Worse yet are the carbon-based units (your employees) who steadfastly refuse to practice safe computing. According to Verizon's 2015 Data Breach Investigations Report, 23 percent of recipients open emails sent by scammers/hackers, and 11 percent download attachments from phishing emails. Results also showed that 50 percent of users click on phishing links within the first hour of being exposed.

Given the depth and breadth of vulnerabilities, much of information security is about risk management. There is some point at which you've done all you can do, within your budget, to secure your data. Then you turn to managing the risk through cyberinsurance.

Your first step is to review your current insurance policy and see what it does cover. If it is indeed the sort of standard policy described previously, it is now time to talk to your insurance agent and explain the kind of coverage you need.

How Much Does It Cost?

Cyberinsurance is not cheap, so be a savvy shopper. The prices remain all over the map, so make sure your insurance agent looks around. There isn't yet a good model for measuring prices, risks, and how to hedge the risks—hence the crazy variation in prices—which are rising steadily, sometimes exponentially, in reaction to the many well-publicized data breaches of the past year.

Some companies still do not offer cyberinsurance, but there are now at least 50. Many have learned that there is gold in the cyberworld to be panned, particularly because almost all states have data breach notifications laws. As of this writing, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

Insurance companies are still gathering actuarial data to help assist in setting prices, but as cyberinsurance is in its adolescence, pricing is volatile. Thank heavens solo and small firms are on the lower end of the spectrum, but it's still costly. In 2015, the cost was roughly $10,000 per $1 million of coverage.

Reuters recently reported that hacking has become such a problem that insurers are now in the process of massively increasing cyber premiums. Insurance companies also are raising deductibles; in some cases by incredible amounts. The list of exclusions is growing, as well, so make sure you read that list carefully.

To minimize risk, insurance companies are submitting self-audits to prospective cyberinsurance customers. They also are taking harsher measures, sending in assessors to get an onsite overview of a law firm's security risks and the premium may be based on how closely the assessors' consequent recommendations are followed. If you do have a self-audit form you are filling out, don't be slipshod and do be candid—your false, misleading, or vague answers will certainly be used against you if you file a claim.

Use a good insurance broker—one who is experienced in procuring cyberinsurance. It is amazing how few brokers have expertise in this area or know which companies to recommend.

Consider being proactive. As an example, considering abiding by the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The more you can show that you are ahead of the curve in protecting confidential data, the better your negotiating posture with the insurance companies, which might earn you a preferred premium rate—not to mention the overall benefits of good risk management.

Very few things are as expensive as investigating a data breach, notifying everyone affected by the breach, and otherwise complying with legal requirements through

notification and the offer of credit monitoring, as well as remediating the problem that caused the breach. This often requires a full-scale security assessment followed by major expenditures to follow all of the recommendations.

Use a good insurance broker—one who is experienced in procuring cyberinsurance. It is amazing how few brokers have expertise in this area or know which companies to recommend. There are certainly companies that have a reputation for denying claims by claiming that they fall under exclusion clauses and others that have a reputation for standing by their customers. Firms are waking up to the potential cost of a data breach, especially if they are in a regulated industry such as finance or healthcare. The Ponemon Institute's 2015 Global Cost of Data Breach Study polled 350 companies in 11 countries and found that malicious attacks take an average of 256 days to discover, while breaches caused by human error take an average of 158 days to identify. The median cost is $3.9 million a year (a 23 percent increase since 2013).

What Will a Prospective Insurer Ask You?

What a prospective insurer will ask varies widely. But be prepared for many, many questions regarding:

- Your network diagram;
- The kind of data you hold, including credit card data, personally identifiable information (PII), Health Insurance Portability and Accountability Act (HIPAA) data, classified data, etc.;
- The nature and frequency of cybersecurity training given to employees;
- Compliance with information security standards;
- Frequency of security assessments—are they conducted in-house or by an independent third party?;
- Policies and plans involving cybersecurity;
- Security currently in place, including firewalls, anti-malware software, data loss protection (DLP) hardware/software, intrusion detection systems (IDS) hardware/software;
- Report of any previous data breaches;
- Security termination procedures upon an employee's departure;
- Physical security of the office(s);
- How the backup is engineered (is it impervious to ransomware?);
- Cybersecurity policies related to vendors and other third parties;
- Do you allow BYOD (bring your own device) or BYON (bring your own network)? If so, how are they managed?;
- Password policies/enforcement; and
- Encryption policies and software/hardware you deploy.

One of the major developments of 2015 was that insurance companies were moving to offer "business interruption" coverage as part of their cyberinsurance policies.

What Coverage Am I Looking For?

There is no consistency between the coverage of the various insurance companies, and they all use different language. It is very hard to determine exactly what you're purchasing, much less make an apples-to-apples comparison.

What if data is somehow transported to a social media site? Are you covered there? What about data breaches in the clouds? It is widely reported that cloud providers tend to have less coverage than might be prudent from the point of view of the law firm that engaged the cloud. Read your cloud vendor's terms of service; it is guaranteed that the provider will try to insulate itself from liability. With 50 percent or more of law firms storing at least some data in the cloud, this is a threshold question to ask.

Not surprisingly, with all the confusion, battles over coverage have wound up in court. In *Zurich American Insurance Co. v. Sony Corp. of America*, Zurich was seeking to absolve itself of any responsibility to defend or indemnify Sony for claims asserted in class actions and other actions stemming from the 2011 hacking of Sony's PlayStation Network. Zurich maintained that the general liability policies it sold to Sony did not apply. Ultimately, the court agreed. If Sony's lawyers didn't know what their insurance covered, imagine the fog a solo or small firm attorney might be in.

One of the major developments of 2015 was that insurance companies were moving to offer "business interruption" coverage as part of their cyberinsurance policies. This is definitely something you want to inquire about.

Another major development of 2015 was the headline "We Don't Cover Stupid"—referring to an insurance

company's refusal to pay a claim when a company that had been breached had not followed "minimum required practices" as spelled out in the policy. This story doesn't involve a law firm, but it is instructive for law firms to read it—there have been a number of insurance companies that say there is no coverage when security of confidential data is sloppy.

The specific suit involves California healthcare provider Cottage Health System and its insurer, Columbia Casualty, which refused to pay up after a breach, pointing to a clause in the policy that effectively said it didn't have to cover the breach because Cottage hadn't followed "minimum required practices" as spelled out in the policy. Many law firms might be vulnerable under such an exclusion.

How Insurers Dodge Liability

Insurers may dodge liability in several ways, including:

- *Not paying retroactively*. Given that breaches can be discovered months after the compromise, law firms should carefully consider when coverage starts.
- *Terrorism/act of foreign enemy exclusions*. Many cyberattacks originate from outside a country's borders, and many of them are believed to be state-sponsored. Depending on the policy's wording, your firm could be left high and dry.
- *Lack of coverage for negligence*. Insurers are starting to cover only data theft, not negligence. If an employee loses an unencrypted laptop with sensitive data, some policies won't cover the breach.
- *Failure to make a timely notification to the insurance company*. Make sure you know when you need to report an incident to your insurer. The clock may be ticking and you don't want to find that your delay means that there are costs you cannot recover—and remember that costs start to mount up quickly after a breach.

In the end, you will have to balance the costs of making security improvements with the cost of cyberinsurance to determine where you are getting the maximum benefit and limiting your risks as much as possible. It is not an easy calculation.

Copyright © 2016 CCH Incorporated. All Rights Reserved.
Reprinted from *The Computer & Internet Lawyer*, December 2016, Volume 33, Number 12, pages 9–11,
with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, *www.wklawbusiness.com*.