CYBER RISK INSURANCE:

Law Firms Need It, Too

By Adrejia L.A. Boutté Swafford
A cybercrime is a criminal act involving a computer and a network. A “cyber incident,” according to the Informative Technology Laboratory at the National Institute of Standards and Technology, is “[a]ctions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.” In this author’s opinion, whether one might become victim to a cybercrime is a matter of when — not if, a point well-illustrated by recent high-profile cyberattacks on the networks of the State of Louisiana and the City of New Orleans, among others. So, why not protect your firm now from the costs and/or expenses of a cybercrime or cyber incident?

“[T]he Ponemon Institute’s ‘2014 Cost of Data Breach Study: United States’ found [that] a company with less than 10,000 records is more likely to be hacked than a firm with more than 100,000 records, in part because smaller firms are less likely to have robust defenses against hackers . . . .” In 2016, the National Association of Insurance Commissioners (NAIC) released a consumer alert which stated that “[d]espite high profile data breaches of large companies, small companies are also targets for hackers as they possess sensitive information but typically have less security than larger companies.” Many juridical persons, i.e., law firms, falsely believe that cybersecurity is an issue strictly for the large companies, but this author believes they are wrong. Although it is true that a larger company might be better financially situated to set up complex and sophisticated security systems and risk management programs, small businesses must also begin factoring this protection into their basic business plans. Part of the answer to how an entity can protect itself from damages associated with a cybercrime is to secure a cyber risk (or “cybersecurity”) insurance policy. “Cybersecurity insurance provides coverage for compromised security or privacy breaches at work.” The NAIC further advised, “[i]f your small business has a disaster recovery plan, consider cybersecurity insurance a part of it.”

Areas of Exposure

Travelers Insurance Co. cites the following top five risks for businesses: 1) “Human Error: Lost and Stolen Laptops and Smartphones,” 2) Hackers, 3) “Spear Phishing: Social Engineering Targeted at Employees,” 4) Extortion, and 5) “Hacktivism: Social and Political ‘Hactivists.’” The NAIC also cites “business interruption from a hacker shutting down a network[,] [d]amage to the firm’s reputation[,] [t]heft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets[,] . . . [t]he cost of monitoring services for people to monitor services impacted by a security breach[,] and lawsuits” as additional types of cyber risks for a business.

According to the 2015 RAND Corp. study, “data breaches” and the “unintentional disclosure of personally identifiable information (PII) stemming from loss or theft of digital or printed information” were reportedly the most common type of cyber event and, aside from an individual’s name and/or address, credit card numbers and medical information were the most vulnerable types of information. The study considered data related to four types of “cyber events”: 1) “data breach,” 2) “security incident,” an “incident involving the compromise or disruption of corporate IT systems (computers or networks) or its intellectual property,” 3) “privacy violation,” the “unauthorized collection, use or sharing of personal information,” and 4) “phishing/skimming,” “instances of individuals committing particular kinds of computer or electronic crimes directly against other individuals or firms.” Malicious intentional attacks far outnumbered those of an accidental basis, totaling around “60% of all incidents.”

Cyber Risk for Law Firms

What is the legal industry’s degree of cyber risk? According to a Texas Lawbook survey, between 2017 and 2018, “four out of five corporate law firms operating in Texas have experienced a ‘cyber incident’ or an actual data breach.” Law firms are targets because they may not be as cyber secure as necessary and because the industry is comprised of small and large businesses, all of which house large amounts of personally identifiable information in the form of medical records, business records, and others. Also, Ansbach, the former general counsel at General Datatech, said that law firms (large and small) are “attractive targets for cybercriminals motivated by factors such as financial gain, activism or national interests because of the secret material and potentially valuable client information they possess.”


[L]aw firms are targets for two general reasons:

1. they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and

2. the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

Further, the ABA’s Oct. 17, 2018, Formal Opinion 483, “Lawyers’ Obligations After an Electronic Data Breach or Cyberattack,” states, in pertinent part:

Data breaches and cyber threats involving or targeting lawyers and
law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.

The TECH REPORT also discusses the fact that, as keepers of volumes of sensitive data (like PII), lawyers have the responsibility to safeguard this information before and after a data breach occurs. It identified the following as specific cyber-related risks of law firms, reported after law firm data breaches — access to sensitive client data; “downtime/loss of billable hours was reported by 41% of respondents;” “consulting fees for repair were reported by 40%;” “destruction or loss of files by 11%;” and “replacement of hardware/software reported by 27% (percentages for firms that experienced breaches).”

According to the ABA, “The FBI has reported that law firms are often viewed as ‘one-stop shops’ for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).” Id.

The Availability

Cyber risk insurance policies have been offered by the insurance industry for more than 20 years. However, many companies did not purchase cyber risk insurance products until “just recently, and even now only 65 percent of ‘large companies’ have some cyber insurance in place.”28 “[T]he threat of a cyber event to small businesses, boutique professional firms, and even personal homes is increasing, and if not insured for cyber risk, could serve that business . . . a crippling blow.”29

The Policy

The cost of premiums may vary but are not unattainable. The premium is based on the “company’s industry, services, type of sensitive data stored/collected/processed, total number of PII PHI records, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue, and more.”30 It is necessary to obtain specific cyber risk coverage because “[t]he standard [Commercial General Liability] policy was never designed to cover lost profits, loss of goodwill, or any intangible losses.”31 In fact, now, “[c]ore commercial policies are more and more often excluding cyber-related claims.”32

The cost of premiums may vary but are not unattainable. The premium is based on the “company’s industry, services, type of sensitive data stored/collected/processed, total number of PII PHI records, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue, and more.”30

It is necessary to obtain specific cyber risk coverage because “[t]he standard [Commercial General Liability] policy was never designed to cover lost profits, loss of goodwill, or any intangible losses.”31

The cost of premiums may vary but are not unattainable. The premium is based on the “company’s industry, services, type of sensitive data stored/collected/processed, total number of PII PHI records, data risks and exposures, computer and network security, privacy policies and procedures and annual gross revenue, and more.”30

Some “[c]yber policies offer ‘breach coaches’ and other benefits that are not available in [other types of liability policies] . . . .”33 Some insurers focus on offering only certain types of coverage. “CNA Financial [Corporation] . . . launched a lawyers’ data breach and network security
endorsement as part of its lawyers’ professional liability policy.” 43 “American International Group, Inc. [AIG] . . . is moving toward explicit coverage for both physical and nonphysical cyber-related risks in its policies.” 44 Generally, a cyber liability policy for an entity might include:

[O]ne or more of the following types of coverage: 40

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputation damage to others when the allegations involve a business or website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings. 41

Overall, the insurer will rely on a business’ “risk-management techniques” when deciding what type of coverage the cyber policy requires, 42 considering things like how employees and others access data systems, “the business’ disaster response plan and evaluate it with respect to the business’ risk management of its networks, its websites, its physical assets, and its intellectual property;” the anti-malware and antivirus software and how often they are run; and the “frequency of updates and the performance of firewalls.” 43

“Coverage can be triggered by the following: [ ] failure to secure data[;] loss caused by an employee[;] acts by persons other than insured[;] and/or loss resulting from the theft or disappearance of private property (such as data that resides on a stolen laptop or missing data storage media).” 44 Unfortunately, many policies fail to cover losses for the unassuming insured — for a number of reasons.

First, the insured may have failed to comply with the policy’s stipulations/prerequisites in the “Application” and/or failed to “maintain minimum cyber security practices,” which can include the requirements to constantly assess and identify security risks and to stay in compliance with governmental and/or industry standard regulations, 46 a provision under some cyber risk policies that can result in no coverage when the insured does not comply. 47

Second, the insured may not have gotten the right cyber risk insurance policy, causing the coverage to fail in part because the insured did not pay attention to the specific endorsements and/or sublimits included. 48 See, New Hotel Monte Leone, L.L.C. v. Certain Underwriters at Lloyd’s of London, et al., 2:16-cv-00061 (E.D. La. 2016). A sublimit:

[b]riefly stated . . . makes a policy worth significantly less if the type of claim or loss is subject to the sublimit. For example, a $10 million sublimit could eliminate $9 million of coverage for the loss at issue. Sublimits are used by several carriers quite frequently in their cyber insurance policy forms. Oftentimes those carriers will sell a policy with an overarching limit but then lower the limits of coverage available for certain types of claims and losses. 49

Keep in mind though, “[m]any carriers are willing to negotiate on the size of a sublimit, sometimes with[ou]t an increase in premium” 50 and some insureds stack sublimits to amount to a desired coverage. 51

Third, the insured may have failed to procure the right policy because it did not consult with an agent and/or broker knowledgeable or experienced in cyber risk insurance. 52 “Getting the right broker is important . . . this may not be the broker you are currently using for your non-cyber risks.” 53 “Share your list of estimated expenses and costs with your broker as he talks the different exclusions that might stop you from making a claim.” 54 Do not rely on what the agent or broker says is covered, read it yourself and, if necessary, retain a colleague who practices in insurance law — preferably cyber risk insurance. 55

**Conclusion**

Purchasing a cyber risk insurance policy is just as practical as buying auto, health or homeowner’s insurance. Although, as U.S. citizens, we have governmental and regulatory bodies in place to help prevent and protect us from a cybercrime or cyber incident, it is not enough. The alternatives to cyber risk insurance simply help us mitigate our exposure. They do not and cannot prevent the inevitable costs and expenses inherent to the occurrence of a cybercrime or cyber incident. Therefore, this author believes law firms need cyber risk insurance.

When procuring a cyber risk policy, always remember to: 1) seek the aid of an experienced cyber risk insurance agent or broker; 2) assess your risks beforehand; 3) pay close attention to the endorsements, sublimits offered (negotiate them if necessary), exclusions 56 and “indemnity agreements;” 57 4) read your policy; and 5) consider consulting with an attorney who is experienced in cyber risk insurance.
FOOTNOTES


7. Id.

8. Id.


10. Id.

11. Id.

12. Id.

13. Id.


16. Id., at 123.

17. Id., at 122.

18. “For example, the theft of laptop or desktop computers containing personal information of employees or customers of a firm, caused either by a hacker or malicious employee. This category also includes the improper disposal or disclosure of personal information (i.e., to a dumpster or website).” Id., at 123.

19. “For example, a denial of service (DoS) attack, the theft of intellectual property, the malicious infiltration (hack) and subsequent cyber extortion of corporate information, or a disruption of business services.” Id.

20. Id.

21. “For example, these crimes would include phishing attacks (wherein criminals seek to harvest account information from users), identity theft (wherein criminals use another person’s information for financial gain), or skimming attacks (where criminals install, e.g., a hardware device over ATM machines in order to copy bank account and bank PIN numbers).” Id.

22. Id., at 123.

23. Id., at 122.


25. Id.


28. Id.

29. Id.


35. The Betterly Report, supra note 28, at 8.

36. Id.


40. Id.

41. Id.

42. Id.

43. Id.


48. Id.

49. Id.


51. Id., at 107.


54. Id.

55. L.D. Simmons, II, supra note 46.

56. “Among the more common exclusions [to a cyber risk policy] are exclusions for dishonest, willful, intentional, fraudulent, and criminal acts of the insured or its employees, war and terrorism, bodily injury and property damage, patent and trade secrets, securities exclusions, and breach of contract exclusions.” See S. Bean & M. Schomburg, Allocation of Losses in Complex Insurance Coverage Claims § 17:4, Cyber and Data Breach Claims (updated December 2016).

57. L.D. Simmons, II, supra note 46, at 32.

Adrejia L.A. Boutté Swafford is an associate at Christovich & Kearney, L.L.P., in New Orleans. She primarily practices insurance defense. She is a member of the Louisiana Bar Journal’s Editorial Board. She reports that she has been a loyal daily contributor to the commuter traffic between Baton Rouge and New Orleans for more than a decade. (alboutte@christovich.com; Ste. 2300, 601 Poydras St., New Orleans, LA 70130-6078)