Cyber Liability Insurance: Is your firm covered?

By: Keren E. McElvy

Eighty percent of the 100 largest law firms have been hacked.[1] In 2014, over 29,000 records were lost or stolen in the United States.[2] The average cost to cover the expenses related to a cyber breach was $5.85 million dollars.[3] Is your firm prepared to handle a cyber attack?

Before thinking your firm is immune, consider three questions. Have you used your computer to send an e-mail containing a client's personal information? Have you used your smart phone to access a document containing confidential data? Have you used your iPad to connect to a server containing your firm's client files? If you answered yes to any of these three questions, have you considered the costs of responding to a cyber attack that intercepts that data? Should that e-mail, document or file be stolen by an unintended recipient, the damage caused and cost to respond can be stifling.

This article is designed to help you determine whether your firm needs cyber liability insurance. Most firms have policies covering property damage, business interruption, and professional liability; cyber liability should be added to the list of insurance policies held by both small and large firms.

1) What is cyber liability insurance?

Cyber liability insurance is designed to cover the costs associated with an electronic security breach. Whether the breach is due to a criminal attack, human error, or a system glitch, cyber liability insurance protects the costs incurred when electronic data is compromised. Data includes personally identifiable information, such as an individual's name associated with his or her social security number, driver's license, credit card number or debit card number.

The first cyber liability policies began to develop in the 1990s. Although coverage had been sought under commercial general liability policies for cyber attacks, the growing risks involved in using

technology to store and send personal identification information presented a need for a more specialized type of insurance designed to cover the growing costs of a cyber attack. In a world where the use of technology was becoming prevalent, companies found themselves exposed to the risks of hackers shutting down their network, human error leaking personal identification information, expenses of credit monitoring services for victims who were affected by the breach, and lawsuits related to the data breach. Professional liability policies which covered website design, content, and services, and commercial policies which covered business injury or property damages, were not enough. Thus, cyber liability policies began to take an individual shape and form.

Cyber liability policies provide a wide spectrum of coverage designed to insure against the risks involved in a cyber attack. Typically, cyber liability policies provide first party and third party coverage. Coverage ranges from policies insuring business interruption from a network being shut down, costs related to cyber criminals who steal personal identification information that can be monetized, costs associated with restoring business assets stored electronically, costs of costumer notification, costs of providing credit monitoring services to victims, and costs of lawsuits relating to the data breach.

Currently, between 25% and 35% of organizations have some form of cyber insurance policy, with the total market value at around $1.7 billion last year.[4] While law firms should be among the top organizations seeking coverage due to the sensitive information kept on behalf of clients, it appears that firms need to be more proactive in buying cyber liability insurance. According to a 2014 survey of 50 law firms,

- 79% said cyber security was one of their top 10 risks in their overall risk strategy.
- 72% said their firm has not assessed and scaled the cost of a data breach based on the information it retains.
- 51% said that their law firms either have not taken measures to insure their cyber risk (41%) or do not know (10%) if their firm has taken measures.

- 62% have not calculated the effective revenue lost or extra expenses incurred following a cyber-attack.[5]

The survey was performed by Marsh, a leading insurance broker and risk adviser. Of the 50 law firms surveyed, 25% employed between 50 to 100 attorneys, 46% employed between 101 to 500 attorneys, and 23% employed between 501 to 1,000 attorneys. These results highlight the importance of law firms understanding why their firms need cyber liability insurance and the need to act on that knowledge.

2) Why does your firm need cyber liability insurance?

Attorneys have access to their clients' private and personal information. Whether the information is learned through an engagement agreement, or the information is learned during the course of the case, attorneys have confidential information that needs to be kept safe. At a minimum, most attorneys have their client's social security number. Whether this information is kept at the office or stored by a third party, the attorney is responsible for the safe-keeping of their client's information. Although an attorney may do all he or she can to keep the information safe, the information is still at risk. Consider the following scenarios.

An employee sending an e-mail with confidential client information could inadvertently type the address wrong, sending the information to an unintended recipient. A hacker could attack your firm's network stealing sensitive client information such as the client's credit card number, drivers' license number, or social security number. An attorney may open an e-mail attachment that appears to come from a client, but is actually a virus which shuts down the office network. Once an event happens which causes a breach, the exposure to costs if your firm does not have cyber liability insurance could be exorbitant.

The average total organizational cost of a data breach is $5.85 million.[6] A company that has a data breach faces the costs of detection of the breach (average cost $417,700); notification to victims of

the breach (average cost $509,237); post-data breach costs such as legal expenditures, identity protection services, and regulatory interventions (average cost $1,599,996); and lost business costs, such as turnover of customers and damage to reputation (average cost $3,324,959).[7]

These numbers come from a 2014 study performed by the Ponemon Institute, which has been studying data breaches and reporting its findings for the past 9 years. The study surveyed 314 companies in 11 different countries, including the United States.[8] The United States was ranked as having the highest total cost associated with a data breach, perhaps due in part to the costs involved in state data breach notification laws.

Almost every state, including the District of Columbia, Guam, Puerto Rico and the Virgin Islands, has a data security breach notification law. The only states that have yet to adopt one are Alabama, New Mexico, and South Dakota.[9] However, the notification requirement is based on where the victim currently resides.[10] Thus, although Alabama does not have a data breach notification law, if a firm is doing business outside the state of Alabama, some form of notification may be required if the victim lives in a state where there is a notification law. While notification laws vary in scope, the general concept is that the laws require a company to notify an individual if their personal identifiable information, such as a social security number or driver's license number, is compromised.

Alabama firms should also keep in mind that a federal notification law may be on the horizon. In light of President Obama's State of the Union address encouraging Congress to enact a uniform federal notification law, both the House of Representatives and the Senate introduced bills that would require companies to notify individuals of a data breach.[11] This would mean Alabamians must be informed of a data breach, regardless of a lack of state law on the subject.

To more fully understand the impact of a data breach, consider the recent cyber attack on Anthem Inc., which was reportedly detected on January 27, 2015. The attack is said to be the largest

data breach to the nation's healthcare sector. The breach impacted around 80 million current and former Anthem customers and employees, and could cost the company over $100 million. Fortunately for Anthem, it has cyber liability coverage; however, it may not be enough to cover the costs of the breach.[12]

One of the measures Anthem is taking to address the affect of the breach is to offer its customers services that provide credit monitoring and identity protection for up to 24 months free of charge. Should all 80 million customers take advantage of that offer, it would cost Anthem over $28 billion according to the monthly price for the services posted on its website.[13]

While most law firms do not service 80 million customers, firms are not immune from the devastating effects of a cyber attack. According to a February 2015 article in Law Technology News, "Larger law firms are starting to recognize the reality of cyberthreats and other data security risks, however many mid-size and small firms are taking the more complacent 'it won't happen to me' approach that is bound to fail them." [14] The article warns, "Law firms and companies that take a more lax approach to data security and risk management in general make them vulnerable to an inevitable breach that will force them to change their ways."[15]

The American Bar Association published an article entitled, "Hackers Are Targeting Law Firms: Are You Ready?" in 2013. The article noted the reasons for hackers' affinity for law firms:

> "[L]aw firms store client information on a single network that is often far less secure than those of the corporate clients they represent. Lawyers often use passwords that are easily cracked. Lawyers are more likely to click on malware-infected phishing email links. And lawyers review sensitive information at unsecure Wi-Fi hotspots. Also, law firms are one-stop shops for hackers. According to the General Counsel of Mandiant, a cybersecurity firm, '[B]y targeting large law firms, hackers can obtain information about hundreds or thousands of companies by breaching a single network.'"[16]

Clients, particularly financial institutions, are beginning to realize the amount of information kept by their attorneys and the value of that information to hackers. Some clients are now requiring

firms representing them to have cyber liability insurance.[17] While every firm has confidential information of its clients, firms that represent financial institutions or industries in the health care sector should be especially concerned in that its files contain highly sensitive information such as credit card and bank account information. As clients become more leery of cyber security, attorneys may be required to purchase cyber liability insurance as a safeguard to ensure that their firms are doing all they can to protect clients' information from cyber attacks.

In determining the risks involved in a cyber attack, firms may look to their general liability policy for coverage. This is probably a mistake.

3) Will your commercial general liability policy cover a cyber attack?

Unfortunately, there is no definitive answer to this question. Court rulings have either been arguably inconsistent or can depend on different factual situations and/or differing CGL policy provisions and exclusions. The correct answer, like many in the legal field, is that it depends. Richard Milone and Genna Steinberg of Kelley Drye & Warren LLP are of the opinion that commercial general liability policies can be a reliable source of coverage for a cyber attack.[18] On the other hand, attorneys at Latham & Watkins opine that traditional commercial general liability policies are unlikely to cover the cost of a breach.[19] In light of the Insurance Services Office, Inc. ("ISO"), change to its standard insurance forms, which excludes cyber breaches from its commercial general liability policy, it seems that a commercial general liability policy is insufficient to provide coverage for the costs involved in a cyber breach.[20]

The first issue to consider is the type of property covered by a commercial general liability policy. In claims alleging lost or damaged electronic data, software, computers, or computer systems, the key issue will be whether the claim falls under the policy's definition of "property damage." Some commercial general liability policies only cover "physical injury or damage" to "tangible" property. If a

court finds that software and data are covered under "tangible" property, a general liability policy may be sufficient, depending on the other provisions in the policy. However, with the costs incurred by a cyber breach, that is not a risk worth taking.

AOL experienced first-hand the problems of having a policy that just covered "tangible" property. AOL's commercial general liability policy did not define "tangible." When AOL suffered a data breach, it sought coverage under its commercial general liability policy. The court held that the damage caused by the cyber breach was not covered under the term "tangible," and ruled in favor of the insurance carrier.[21] On the other hand, the Court of Appeals of Minnesota found that a commercial general liability policy was ambiguous as to whether "tangible" property included coverage for a computer tape containing data belonging to a third party, and ruled in favor of coverage.[22]

Whether a court will consider electronic data "tangible" property is just one of many issues that can arise when relying on a commercial general liability policy. Another issue to consider is a claim for defense and indemnification. In 2011, Sony Corp. of America and Sony Computer Entertainment America suffered a breach where over 77 million user accounts were hacked, costing Sony approximately $2 billion.[23] The insurance company denied Sony's defense and indemnification claim, and filed suit seeking a ruling that it did not have to defend Sony against any data breach claims. In 2014, the New York Supreme Court determined that the insurance company had no duty to defend. Specifically, the court found that the policy covered material published directly by Sony, and not the third party who stole the data.[24] The Sony case recently settled. One blogger calls the case a "Super Bowl ad for cyber liability insurance" and remarks that "Sony showed that companies cannot look to general liability policies to cover data breaches. They need to get cyber insurance."[24.5]

In May 2014, the ISO endorsed several exclusions relating to disclosure of personal information in its commercial general policies.[25] One of those exclusions states,

> *"'CG 21 06 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – With Bodily Injury Exception)* — excludes coverage, under Coverages A and B, for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.'
>
> The endorsement also provides that the exclusion will apply even if damages are claimed for notification costs, credit monitor expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by the named insured or others with respect to that which is subject to the exclusion. This endorsement also includes a limited bodily injury exception arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[26]

This exclusion, and the other exclusions endorsed by the ISO, makes it less likely that a general liability policy would provide coverage. In addition, the ISO has developed separate policies for data breach and other cyber-related exposures.[27] While some have opined that the fact that ISO has published exclusions to their commercial general liability policy indicate that the previous commercial general liability policy covers cyber breaches, that is probably not an argument worth risking in court.[28] The best choice is to procure cyber liability insurance that specifically covers the damage incurred in a cyber attack.

4) How can you protect your firm from the damages of a cyber attack?

There are many different cyber insurance policies are available. It is important to assess the risks and needs of your firm, then to consult with a broker to determine the best fit for your firm.

Robert Berman of Cobbs Allen, an insurance broker who helps clients determine the best cyber liability policy for their firm, explained the different variables that should be considered in determining the right policy and price for a firm's cyber liability coverage. As expected, the larger the firm, the higher the price. He also explained that the practice areas of the attorneys in the firm affect pricing. For example, a firm that mainly deals with collections has more exposure because it is likely to have credit card and debit card account numbers of its clients. He also discussed the different coverage options. In

regard to notification costs, some policies cap the cost in terms of a dollar amount, while others cap the cost in terms of the number of records compromised.

Another coverage option would be to have business interruption coverage. This coverage would protect any exposure faced by a firm if its website is shut down. He explained that this is an area where there would probably not be a lot of exposure for a defense firm, since a firm is not likely to suffer a huge loss if its website is down for a day. He added that most policies also have a public relations component and a forensic component.

In a firm of 25-30 insurance defense attorneys, he said the limit of liability would be $1 million. The defense cost would be included in the cost of the insurance. For a $1 million dollar policy, the premium would be around $2,000 a year.

Cobbs Allen is part of the Chubb Group of Insurance Companies which insures over 95% of the top 200 U.S. law firms. Like most cyber insurance policies, Chubb's CyberSecurity policy covers first party and third party losses. The policy covers privacy notification and crisis management expenses, reward expenses arising out of a covered wrongful act or expense, E-business interruption and extra expenses, E-threat expenses resulting from the insured surrendering funds to a person who makes a threat, and E-vandalism expenses resulting from the destruction of data owned by the insured.

Most cyber insurance policies cover first party and third party losses. For example, Travelers' CyberRisk policy offers ten separate cyber insurance coverages, designed to address the broad array of cyber security exposures emerging in today's world. The policy covers first party losses, including: crisis management event expenses, security breach remediation and notification expenses, computer program and electronic data restoration expenses, computer fraud, funds transfer fraud, e-commerce extortion, and business interruption and additional expenses. The policy also covers exposure under

third party losses, such as network and information security liability, communications and media liability, and regulatory defense expenses.[29]

When negotiating a cyber liability policy, there are some key considerations to keep in mind. Analyzing your potential exposure is the first step. One way to analyze your exposure is to hire a forensic firm to perform a forensic analysis of your law firm's exposure to cyber risks. Once you receive the report, "Other key considerations include whether the company has overseas operations, whether the company has call centers, the extent of the company's internet operations and the company's reliance on cloud computing."[30] These factors will help determine the risk of your firm's data, and help to provide the best coverage for your practice.

5) Conclusion

After considering the risks involved in failing to procure coverage for a cyber breach, the advantages of purchasing cyber liability insurance are well worth the cost. Last year, Cobbs Allen issued approximately 50 cyber liability policies. Less than 10% of those policies were issued to firms that had around 25-30 attorneys. This data suggests that many Alabama attorneys need to evaluate their exposure to cyber risks. You would never leave the door to your firm unlocked after closing time, why leave data exposed to cyber threats 24/7? According to ComputerWeekly.com, "Data breaches are now a fact of life together with taxes and death."[31] If your firm is not prepared for a cyber attack, now is the time to do so. Conducting a forensic analysis of your firm's exposure to cyber threats, addressing those security issues, and procuring cyber liability insurance for coverage in the event of a cyber attack are crucial to protecting your clients' information and your firm from the extensive costs of an electronic data breach. Relying on your firm's commercial general liability policy for coverage is not enough. Procuring coverage through a cyber liability policy is the best decision to ensure coverage for your firm, should an electronic data breach occur.

[1] Marsh, *More Cyber Preparedness Needed, According to 2014 Law Firm Cyber Survey*, MARSH USA (January 15, 2015), available at http://usa.marsh.com/NewsInsights/ThoughtLeadership/Articles/ID/43529/More-Cyber-Preparedness-Needed-According-to-2014-Law-Firm-Cyber-Survey.aspx (last visited February 23, 2015).
[2] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis* at 1, PONEMON INSTITUTE LLC (May 2014), *available at* http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03027usen/SEL03027USEN.PDF (last visited February 23, 2015).
[3] *Id.*
[4] Cath Everett, *Is cyber-insurance an enterprise essential in a data breach age?* DIGINOMICA (February 3, 2015), *available at* http://diginomica.com/2015/02/03/cyber-insurance-enterprise-essential-data-breach-age/ (last visited February 23, 2015).
[5] Marsh, *More Cyber Preparedness Needed, According to 2014 Law Firm Cyber Survey*, MARSH USA (January 15, 2015), *available at* http://usa.marsh.com/NewsInsights/ThoughtLeadership/Articles/ID/43529/More-Cyber-Preparedness-Needed-According-to-2014-Law-Firm-Cyber-Survey.aspx (last visited February 23, 2015).
[6] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, PONEMON INSTITUTE LLC (May 2014), *available at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03027usen/SEL03027USEN.PDF* (last visited February 23, 2015).
[7] *Id.*
[8] *Id.*
[9]National Conference of State Legislatures, "State Security Breach Notification Laws," *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited February 23, 2015).
[10] AmWINS Group, Inc. , Client Advisory, *What is Cyberliability?* AMWINS GROUP, INC., *available at* http://www.amwins.com/SiteCollectionDocuments/Client%20Advisories/Client_Advisory-What-Is-Cyberliability.pdf (last visited February 23, 2015).
[11] Covington & Burling LLP Privacy and Data Security Practice Group, *Data Breach Notification Bills Introduced in House and Senate*, THE NATIONAL LAW REVIEW (February 4, 2015), *available at* http://www.natlawreview.com/article/data-breach-notification-bills-introduced-house-and-senate (last visited February 23, 2015).
[12] Charlie Osborne, *Anthem data breach cost likely to smash $100 million barrier*, ZDNET (February 12, 2015), *available at* http://www.zdnet.com/article/anthem-data-breach-cost-likely-to-smash-100-million-barrier/ (last visited February 23, 2015).
[13] David Robinson, *This is how much a cyber security breach could cost Anthem*, ALBANY BUSINESS REVIEW (February 13, 2015), *available at* http://www.bizjournals.com/albany/blog/health-care/2015/02/how-much-a-cyber-security-breach-could-anthem.html (last visited February 23, 2015).
[14] Erin E. Harrison, *'Fundamental Shift' in Law firms' Cybersecurity Efforts*, LAW TECHNOLOGY NEWS (February 5, 2015), *available at* http://www.legaltechnews.com/id=1202717094272/Fundamental-Shift-in-Law-Firms-Cybersecurity-Efforts (last visited February 23, 2015).
[15] *Id.*
[16]Stacy Berliner, *Hackers Are Targeting Law Firms: Are You Ready?* AMERICAN BAR ASSOCIATION (August 27, 2013), *available at* http://apps.americanbar.org/litigation/committees/womanadvocate/articles/summer2013-0813-hackers-are-targeting.html (last visited February 23, 2015).
[17] American Law Institute CLE, *Law Firms Need to Protect Themselves with Cyber Insurance*, AMERICAN LAW INSTITUTE CLE (May 7, 2014) *available at* http://www.morethancle.org/law-firms-need-protect-cyber-insurance/ (last visited February 23, 2015).
[18] Richard D. Milone and Genna S. Steinberg, *Insurance coverage for cyber liability*, KELLEY DRYE & WARREN LLP (December 15, 2014), *available at* http://www.metrocorpcounsel.com/articles/30998/insurance-coverage-cyber-liability (last visited February 23, 2015).
[19] Latham & Watkins Client Alert, *Cyber Insurance: A Last Line of Defense When Technology Fails*, LATHAM & WATKINS INSURANCE COVERAGE LITIGATION PRACTICE (April 15, 2014), *available at* lw-cybersecurity-insurance-policy-coverage.pdf (last visited February 23, 2015).
[20] *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INSURANCE JOURNAL (July 18, 2014), *available at* http://www.insurancejournal.com/news/east/2014/07/18/332655.htm (last visited February 23, 2015).
[21] *America Online, Inc. v. St. Paul Mercury Insurance Co*., 207 F. Supp.2d 459, 462 (E. D. Va. 2002).
[22] *Retail Systems, Inc. v. CNA Insurance Companies*, 469 N.W.2d 735, 737 (Minn. Ct. App. 1991).
[23] Young Ha, *N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation*, INSURANCE JOURNAL (March 17, 2014) *available at* http://www.insurancejournal.com/news/east/2014/03/17/323551.htm (last visited February 23, 2015).
[24] *Id*.

[24.5] Joshua Mooney, Sony Data Breach Coverage Litigation Settles, THE COVERAGE INKWELL (April 30, 2015), *available at* http://thecoverageinkwell.com/sony-data-breach-coverage-litigation-settles/ (last visited May 5, 2015).
[25]*ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INSURANCE JOURNAL (July 18, 2014), *available at* http://www.insurancejournal.com/news/east/2014/07/18/332655.htm (last visited February 23, 2015).
[26] *Id*.
[27] *Id*.
[28] Judy Greenwald, *Insurers fight to bar cyber coverage under commercial general liability policies*, BUSINESS INSURANCE (October 26, 2014), *available at* http://www.businessinsurance.com/article/20141026/NEWS07/141029850 (last visited February 23, 2015).
[29] Travelers CyberRisk Policy CYB-3001 Ed. 07-10, THE TRAVELERS INDEMNITY COMPANY (2010), *available at* https://www.travelers.com/business-insurance/management-professional-liability/documents/CYB-3001.pdf (last visited February 23, 2015).
[30] Latham & Watkins Client Alert, *Cyber Insurance: A Last Line of Defense When Technology Fails*, LATHAM & WATKINS INSURANCE COVERAGE LITIGATION PRACTICE (April 15, 2014), *available at* lw-cybersecurity-insurance-policy-coverage.pdf (last visited February 23, 2015).
[31] Sarb Sembhi, *An introduction to cyber liability insurance cover*, ComputerWeekly (July 29, 2013), *available at* http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover (last visited February 6, 2015).