Everything You Need to Know About Cyber Liability Insurance But Never Knew to Ask

By JoAnn L. Hathaway

Why you need cyber liability insurance

Law firms as targets

The word is out: cybercrime is everywhere. As a result, businesses are becoming much more knowledgeable about how to protect their data. Subsequently, cybercriminals are focusing on easier-to-exploit organizations, and law firms are being targeted at an alarming rate.

Law firms routinely handle highly valuable and sensitive information, and often do not have sophisticated security in place. Accordingly, their defenses are down and they become easy targets.

Lack of knowledge and awareness about the cyber risks they face and the potential impact of an attack have kept many law-firm managers from purchasing cyber liability insurance policies. Some believe they have adequate coverage for cyber risks under their firm's current insurance policies. However, other policy types with add-on endorsements often offer only a minimal amount of cyber coverage as compared to a dedicated cyber liability insurance policy.

It is recommended that you work with your insurance agent to review your current policies to understand what cyber insurance coverage you may have and to identify any gaps in coverage. Understanding the many exposures that exist today can be somewhat daunting, but seeking guidance from a professional can go a long way toward ensuring you have the protection you need for both your law firm and your clients.

Understanding basic cyber liability insurance coverage

Insurance coverage for first-party losses

This insurance covers costs and expenses resulting from a breach response, which normally includes costs incurred to investigate and remedy a security breach. Examples of costs involved with a breach include:

- Attorney and forensic examiner fees
- Public relations firm fees to restore reputation and mitigate damages
- Regulatory fines
- Business interruption loss
- Payments for cyber extortion
- Electronic information restoration
- Identity theft resolution services fees
- Notification of breach costs
- Credit file monitoring costs
- Out-of-pocket operating/replacement costs

Insurance coverage for third-party losses

This insurance covers losses arising from claims asserted against an individual or entity for an unintentional breach of information, network security damage, media liability, intellectual property infringement, and costs associated with regulatory proceedings and legal violations.

Common payments made under this coverage include those for damage judgments or settlements, defense and claims administration costs, and payments made under the consumer redress fund in a regulatory action.

Working your way to coverage

Cost

The cyber insurance market is less developed than most other lines of insurance, and there isn't as much historical information to rely on to create a standard premium estimate. Also, as is the case with many lines, because there are so many variables in coverage and options from which to choose, it is difficult to quote average premium numbers.

The good news is that many carriers are entering the cyber insurance marketplace, resulting in a soft market. This means that potential policyholders are able to pick and choose between insurance carriers, and premiums are more competitive.

Many factors affect a premium quote, including:

- **Risk management—**If a firm can demonstrate it has a strong network and safeguards in place to include both by way of policies and procedures and human resources support, a carrier may provide credit to its underwriting formula and arrive at a more favorable premium when compared to a firm without optimal technology oversight.
- **Liability limit and deductible—**The higher the liability limit purchased, the higher the premium. Conversely, the higher the deductible purchased, the lower the premium.
- **Claims history—**If a firm has a claims history, the claims will be factored into the premium quote. A carrier will also look to the facts and circumstances giving rise to the claims to determine if

---

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content or call our Helpline at (800) 341-9715 to speak with JoAnn Hathaway or Diane Ebersole, Practice Management Advisors.

they suggest weaknesses and poor network security.

- **Firm Footprint—**Firms that practice globally are subject to risks that don't affect firms practicing only locally. Different geographic locations face different exposures and privacy laws. A firm's geographic spread is evaluated during the underwriting process, and the variables are considered.

The application

Completing an application for a cyber liability insurance policy can be a rather daunting task. Questions call for information not usually required for other lines of insurance. As one would imagine, the application includes many technical questions, which may call for a team of individuals to respond. These questions typically cover the following areas.

Computer and network security

The prospective insurer will ask who in your firm is responsible for information security and the role of the person he or she reports to.

With regard to the firm's computer systems, you will need to provide information about the existence of backup systems, business continuity and disaster recovery plans, and incident response plans for network intrusions and virus incidents.

The carrier will also want to know if you have:

- Up-to-date, active firewall technology
- Patch management procedures
- Multifactor login for privileged access
- Remote access limited to VPN
- Updated antivirus software on all computers and networks
- Intrusion detection software
- Valuable/sensitive data backup procedures and procedures to test or audit network security controls

You should also be prepared to provide information on personnel policies and procedures and vendor management. Specifically, you will be asked if:

- Employees are trained in security issues and procedures
- Computer access is terminated when an employee leaves the firm
- Procedures are in place for creating and updating passwords
- Background checks are conducted on prospective employees
- Service providers are required to demonstrate adequate security policies and procedures
- Contracts with service providers include hold harmless and indemnification agreements
- The firm is using a cloud service provider and, if so, its identity

Information security

The prospective insurance carrier will also inquire about what type of data the firm collects, receives, processes, transmits, and maintains as part of its business activities. This includes:

- Credit and debit card data
- Medical information
- Social Security numbers
- Employee/human resources information
- Bank accounts and records
- Intellectual property of others

Once the data types are identified, you will be required to provide the number of individuals for whom you handle this data.

Additionally, the carrier will ask if your firm is compliant with HIPAA and payment card industry standards regarding data security, and whether you encrypt data, including data at rest, in transit, and on mobile devices.

Website and content information

The carrier will seek specific information about your website. You will be asked whether your firm has a written intellectual property clearance procedure for web content.

You will also need to answer if your firm has a formal policy or procedure in place to:

- Avoid the posting of improper or infringing content
- Edit or remove controversial, offensive, or infringing content from material distributed or published by or on behalf of your firm
- Respond to allegations that content created, displayed, or published by you is libelous, infringing, or in violation of a third party's privacy rights

Loss information

Not surprisingly, you will need to supply information on the firm's loss history. This may be limited to a specific period. In addition to answering questions about each loss, you should be prepared to provide documentation with details about each claim and any corrective measures the firm has undertaken to ensure such a loss does not occur in the future. Audited or financial statements may be requested if the firm is seeking higher limits of liability protection.

Warranty statements

Most cyber liability insurance policy applications contain warranty statements, meaning that when you sign the application, you agree that the information provided is accurate and complete. It is in your firm's best interest to ensure that the questions are answered fully and the information is current. Failure to provide accurate or complete information could result in denial of a claim, even if there would have been coverage under the policy.

Dissecting the cyber liability insurance policy

The declarations

The declarations page outlines the terms of coverage, identifies the policy period, and states your limits and deductibles by insurance part. It is common to have more than one deductible and more than one limit/sublimit as a result of the different types of coverage in the policy (first party and third party).

Insuring agreement

The insuring agreement describes what the policy covers. Ideally, your policy will provide coverage for both first-party and third-party losses. This part of the policy can be relatively short. For example, I reviewed one policy that set forth the insuring agreement for first-party and third-party losses in only 10 short paragraphs, with an average paragraph length of three

lines. When sitting down to read a policy (which *everyone* who seeks coverage should do), a potential insured will find that the "heavy lifting" often comes under the definitions section.

Definitions

The definitions section defines the terms and phrases set forth in bold throughout the policy. The 10 paragraphs referenced in the insuring agreement above contained 34 terms and phrases in bold, driving home the importance of carefully reading and fully understanding the pages of definitions in the specimen policy under review. Failure to do so would leave a prospective insured in the dark and uninformed about what is or isn't covered under the policy.

Exclusions

A cyber liability insurance policy contains an exclusions section, which should clearly describe what is and isn't covered under the policy. More is better here—a statement that may be confusing to some.

A number of insurance carriers do not list what they consider to be obvious exclusions, believing the insuring agreement and other policy provisions describe what is insured under the policy. Since reading and fully understanding a cyber liability insurance policy can be an intimidating task, fully fleshed-out exclusions can be very helpful to prospective insureds.

Defense and settlement

The policy describes the relationship between the insured and insurer as it pertains to the control of the defense and settlement of a claim. As with the policy in its entirety, this provision should be reviewed carefully to fully understand the authority you as the insured have under the policy.

It is common for a cyber liability policy to be written on a "non-duty to defend" basis, which allows the insured to manage and control the defense of claims. Usually, these types of policies let the insurer have a say in important decisions.

There are certainly policies in the market where the insurer has a duty to defend, even if the claim has no perceived merit. When this is the case, it is best to find a policy that allows you some input regarding the selection of defense counsel.

It is common for larger law firms with the staff and departments to manage complex cyber liability claims to prefer a policy written on a non-duty to defend basis. Conversely, solo and smaller law firms tend to want a policy which gives the insurance carrier the burden of managing the defense.

Some carriers issuing non-duty to defend policies reimburse their insureds for defense costs after they are incurred, while others provide an advance payment for these costs. If you are not in a position to pay these and wait for reimbursement by your carrier, select a policy that provides for advancement of defense costs.

A cyber liability insurance policy commonly requires the written consent of the insured before settling a claim. However, this routinely comes with conditions. One such example is that if the insured withholds consent to settle for an amount the insurer recommends, the insured will be solely responsible for 30 percent of all defense costs incurred after the date the insured refused to consent to the settlement and 30 percent of all loss payments paid in excess of the settlement offer.

Liability limits/self-insured retention

An aggregate liability limit is provided for under a cyber liability insurance policy along with sublimits for each first-party and third-party loss. In addition, a deductible applies for each coverage part. This generally varies depending on the size of the policy and the firm being covered.

Conditions

In very general terms, this policy provision sets forth what you are required to do to remain insured under the policy, and to help ensure coverage will be available for you in the event of a claim. Examples of some of these conditions are:

- The timely payment of premiums and self-insured retentions
- In the event of a loss, taking reasonable steps to protect your firm from further loss or damage
- Cooperating in a data breach investigation
- Providing your insurance carrier with proof of loss in a timely manner

Other insurance coverage

This provision describes how the policy will apply to a loss or losses in the event you have other effective insurance coverage in place that may also apply to a loss.

Territory

The territory section in a cyber liability policy identifies exactly where in the world coverage would be afforded to you for a loss. The broadest policy provides coverage for acts initiated anywhere in the world.

Conclusion

These are some of the main policy provisions of a cyber liability insurance policy. Because there is no standard policy form—meaning coverage offered by one insurer may greatly differ from another—policies you review may have differing coverages from those identified here. Given the complexities and variables contained in cyber liability insurance policies, it is recommended that anyone seeking insurance coverage consult with an experienced insurance agent or broker and an insurance attorney whose practice area concentration focuses on cyber liability insurance policy reviews. ■

JoAnn L. Hathaway is a State Bar of Michigan practice management advisor. Previously, she worked as a legal liability claims director and risk manager. She is an Adobe Acrobat certified expert, is certified in LexisNexis Time Matters and Billing Matters software, is a licensed insurance agent, and holds the designation of registered professional liability underwriter. JoAnn is a frequent speaker on law firm technology and risk and practice management topics.