CYBERSECURITY ALERT:

TIPS FOR PURCHASING CYBER INSURANCE

ISSUED BY THE

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

OF THE

NEW YORK STATE BAR ASSOCIATION

July 6, 2020

Opinions expressed are those of the Committee preparing this Cybersecurity Alert and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

Ronald J. Hedges
Dentons USA

EX OFFICIO, CO-CHAIR

Mark A. Berman
Ganfer Shore Leeds & Zauderer LLP

VICE CHAIR

Shawndra G. Jones
Epstein Becker Green

COMMITTEE MEMBERS

Seth Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Sanford Strenger
Ronald P. Younkins

AUTHORS OF THIS ALERT

Mike Mooney
Laurie Kamaiko

CONTRIBUTOR

Gail L. Gottehrer

INTRODUCTION FROM THE CO-CHAIRS

As a result of the dramatic increase in cyberattacks that we have seen since the start of the COVID-19 pandemic and the risks associated with lawyers working remotely and using unfamiliar technologies, cyber insurance has become an important consideration for many law firms. For lawyers who may not be familiar with cybersecurity, the thought of completing a cyber insurance application and deciding how much coverage to purchase can be intimidating.

Continuing our focus on providing practical, understandable, and timely cybersecurity resources to our community, the Committee on Technology and the Legal Profession has put together this Alert, to help lawyers know what to expect when applying for cyber insurance and to provide them with tips to increase their comfort level with the process. Like our other Alerts, it is concise and easy to read.

The Committee thanks Laurie Kamaiko, Esq. and Mike Mooney, both members of our Cybersecurity Subcommittee, for preparing this Alert and sharing their expertise and insights on this important topic.

Tips for Purchasing Cyber Liability Insurance

Buying a new line of insurance, particularly Cyber Insurance, may seem like a daunting task. Below are a few checklists that can help attorneys who may be unfamiliar with the process of applying for cyber liability insurance.

The Application Process

1. The application usually consists of 12-15 questions.
2. Have a general idea of how many client records you have
3. Provide carrier with Law Firm Size (number of staff and number of attorneys)
4. Provide carrier with Law Firm Revenue
5. Disclose any previous losses relative to hacks or breaches

Questions About Your Risk Management Procedures

In order to get the best Terms and Conditions, you will need to be able to answer "yes" to the following questions:

1. Are your computers set up to automatically download and install updates to the operating system?
2. Do your email systems require dual factor authentication?
3. Have your computers been updated to use DNS services with advanced security?
4. Have administrative privileges been restricted on each computer?
5. Have you, and the attorneys and employees at your firm who have financial and accounting responsibilities, completed social engineering training?

Questions About Phishing and Social Engineering

Because of the rise in phishing attacks, insurance carriers generally ask the following questions as part of the application process:

1. Have the employees at your firm who have financial and accounting responsibilities completed social engineering training?
2. Does your firm send and receive wire transfers? If the answer to this question is "yes," does your wire transfer procedure include:
    a. A wire request documentation form?
    b. A protocol for obtaining proper written authorization for the wire transfer?
        i. Use call-back verification
        ii. Dial a number you already have on file
    c. A separation of authority protocol?

d. A protocol for confirming all payment and funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment of funds transfer instructions/request was received?

e. A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the payment of funds transfer instructions/request was received?

    i. Use call-back verification

    ii. Dial a number you already have on file

    iii. Verify changes

    iv. Investigate unique requests

    v. Be alert

Note: If your answer to any of these questions is "no," it does not mean that your application for coverage will automatically be denied. Some carriers will ask you to require members of your firm to participate in training on proper wire transfer processes that the carrier will provide.

Other Things to Consider

1. Do you handle matters that require you to hold or have access to particularly sensitive information of clients, such as:
    a. Information on client assets for trusts and estates matters
    b. Medical records
    c. Intellectual Property and trade secrets
2. Do you have backups of the data on your computer systems that are separate from your network that you can use if your network is shut down (such as in response to a ransomware attack)?
3. Do you have an Incident Response Plan outlining the steps you will take if you suspect you have been affected by a data breach, ransomware attack, successful phishing attack or other cyber incident?
4. Does your insurance broker regularly place cyber insurance so she can help you identify the appropriate scope of coverage and limits for you?

Purchasing Cyber Insurance

- Purchasing a cyber insurance policy should be done through a broker.
- Be very careful when selecting a broker.
    - Just like we advise clients to select an attorney based on their specialization in a particular area of practice, this holds true in selecting a cyber insurance broker.
    - You want a broker that understands the policy forms and coverages, and can advise you on the appropriate limits and deductibles you should have, based on the size of your firm and area of practice.
    - The terminology on this line of coverage can vary from carrier to carrier, which makes it important to have a broker who is knowledgeable about the forms.
- Explore your broker's risk management capabilities.
    - A good broker should be able to provide you with articles, advisories, guides, and other risk management materials that can help you mitigate risk and protect your billable hours.
    - In general, cyber liability insurance is well priced for the benefits it provides and significantly less expensive than a firm's legal malpractice insurance, although as losses increase, the price for cyber insurance will also increase.

Common Risk Management Services Included with Cyber Insurance

- Employee training
- Breach coach
- IT forensic specialists
- Claims and advice hotline
- Online knowledge resource center
- Email news and alerts