CYBERINSURANCE

Ellen Freedman, CLM

We've heard a lot about data breaches. Most have been costly. Some have resulted in lawsuits. Although there isn't a long history of payoffs, insurance companies have responded with a concerted effort to better control risks. As a result, coverage for data breaches and related events have been removed from coverage in most multi-peril policies. Companies must now purchase this insurance through a separate insurance policy or rider. Law firms have begun contacting me for guidance on how to determine if they have risk, how much that risk might be, and whether or not they should purchase cyber insurance to mitigate the risk.

Cyberattacks of small and midsize businesses are on the rise. Law firms of all sizes are targets. Social engineering frauds are steadily increasing, according to the FBI. And let's remember that attacks come from a variety of sources, from a malicious current or former employee, to phishing scams, telephone hacking, and malware. Keep in mind that breaches aren't always the result of a cyber-attack. Many data breaches stem from something as simple as the loss or theft of an unencrypted laptop, smartphone or USB stick.

Targets of attacks include your trust accounts, as well as valuable intellectual property or sensitive information regarding employees, clients, or even vendors. The losses from a successful breach may include the actual loss from theft and fraud, plus items such as forensic investigation, business interruption, extortion fees —think crypto locker—computer data loss and restoration, replacement of computer equipment, and loss of clients. Depending on what information is exposed, there may be additional losses associated with litigation and regulatory penalties, regulatory response, notification costs, crisis management, credit monitoring, public relations for brand and reputation damage, and 3rd party claims for liability for breach of privacy.

Beware of exclusions!

Some policies include a "Portable Electronic Device Exclusion." This means that if the device leading to a cyber breach is portable, the policy could exclude coverage completely for any resulting loss. This exclusion could be devastating for a

law firm, where smartphones, tablets and laptops are routinely used. Some cyber policies exclude coverage for data an organization has entrusted to a third-party vendor who is breached. As firms increasingly move data to the cloud, it's essential that firms not assume that the cloud vendor has adequate coverage to cover the firm's losses in the event of a breach. You need to make sure you have your own coverage in place. Some policies exclude coverage for employee-owned devices that are the cause of the breach. This would have huge implications for a firm's BYOD policies and protections.

The first step to determine how much insurance you need is to determine what you stand to lose in the event of a data breach or cyber-attack. This involves an inventory of the types of information and information systems you have, and an assessment of the magnitude of harm expected to result from having that information compromised, or from your information being unavailable for some length of time. Consider the size of your firm, and the type and amount of data your firm manages. Additional factors to consider include how much money in aggregate you have in your trust accounts. Plus, what your firm's practice areas are. This will determine the sensitivity — potential theft value — of the information found in your client's documents.

The Ponemon Institute estimates that the average cost of a data breach is $201 per lost record. A policy for $1 million in coverage covers a data breach of approximately 5,000 lost records. This cost includes services which are typically uninsurable, such as lost customer business. The total amount of insurable costs may, some postulate, be as low as $100 per record.

The Net Diligence 2014 Cyber Claims Study examined actual insurance policy payouts for claims. They reported that the average per record cost was $956.21. Because they only examined payouts, there is no determination of the actual loss per record of policyholders.

I was shocked to find an article in Inc. in which Matt Cullina, CEO of IDT911, (which helps customers avoid identity theft and other data exposure risks), was quoted as recommending a $50,000 policy as adequate for most small companies. (That covers just 248 lost records, using the data from Ponemon Institute!) He further recommends that getting a cyber-liability rider added to a standard insurance policy will cost far less; possibly one tenth as much as a standalone policy for comparable coverage. I'm skeptical. I find the dollar recommendation unrealistically low, and we know not all insurance policies are alike. Inclusions and exclusions, as well as definitions, will ultimately determine whether the policy is as valuable as it appears.

With such a wide range of predicted costs per record lost, it's no wonder potential policyholders are left scratching their heads in wonder. Some firms are "plucking numbers from a cloud;" a method reminiscent of when valuable papers coverage was first available to policyholders. If your firm purchases cyber insurance it must place a value on the firm's risk. This is definitely the most difficult aspect of the endeavor. The underwriting process itself can help a firm identify security gaps and ways to lower risk. Plus, many cyber insurance policies provide risk mitigation tools, and significant incident response assistance. The bottom line, sadly, is that it's far easier to know how much coverage you need *after* a breach than before.

Right now it's a competitive marketplace for cyber insurance, often referred to as a "soft" market. There is the ability to customize your policy so you only buy the coverage you really need. And prices vary widely from one carrier to the next. There are some "best practices" you can implement at your firm to lower your premium. Some examples are to eliminate unnecessary data, regularly change passwords, avoid sharing logins and passwords, update software immediately, provide regular employee education on risky behaviors, and audit user accounts on a regular basis. If you can document that these policies are in place and followed consistently, you may see your premium quote reduced.

A version of this article originally appeared in the August 8, 2016 issue of the Pennsylvania Bar News.

Freedman Consulting, Inc.
(215) 628-9422