Freedman Consulting, Inc.
CHANGE . . . RESULTS . . . SUCCESS

CYBERSECURITY INSURANCE TIPS

Ellen Freedman, CLM

I don't know about you, but I really enjoy attending most seminars and have found that some of the free seminars are the very best ones. Even though they often don't offer CLE credit, the learning takeaways can be significant. Frankly, even if I come away with just one or two nuggets of gold I can put to immediate use, it's worth my time.

On March 13, I attended "Navigating Cyber Insurance for Legal Professionals," presented by Partner and Senior Vice President of USI Affinity Mike Mooney. It was a fast-paced webinar loaded with good nuggets. You have probably been hearing the words "cybersecurity" and "cyber breach" way too often. Still, we need to take the time to learn more on this topic.

Every single day, new threats are created and released, so we need to stay ahead of developments, keep educating ourselves and our colleagues and work with our vendors to continue reinforcing the gates that keep the bad actors outside our computing environment.

The number of potential cyberattacks has increased exponentially. Phishing emails, emails with malware attached and malicious links embedded, are now arriving eight to ten times a day – even after mail filtering or blacklisting every single domain or sender who sends me something unwanted or dangerous. Many appear to come from vendors and even clients I regularly communicate with.

Cyberattacks are getting so "real" that it's increasingly hard to know if an email is legit or not without examining each one. So, about a half dozen times a day, I go into my contacts and send an email to someone asking if they sent me the email I deemed suspicious or if it was another cyberattack attempt. I never reply directly to the email because there's likely one character that's different from their normal email address that I might not have noticed that would give away the cyberattack disguise.

Every single channel of communications is under attack. Dozens of malicious smishing text messages arrive each day. Phony connection requests on Facebook, hundreds of vendors trying to lighten my wallet weekly and phony private messages through Facebook Messenger and LinkedIn. Oh, and don't even get me started on the phone calls and fake voicemails.

I have to be aware of these fake messages and calls for myself, but for you, too, because I get frequent calls on the hotline from people wanting to know how to protect themselves from scam or spam calls/messages. "Am I less at risk if I do A instead of B?," "I read about what happened to firm ABC, can that happen to me? How do I prevent it?," "Do I need cyber insurance? And if so how much?" or "What makes one policy worth more than another?" are all frequently asked questions I get on the hotline,

Although I can confidently answer the questions about professional liability insurance, questions like these prompted me to sign up for the USI webinar.

The most important information presented at the USI webinar was a clear understanding of what the critical coverage issues are. USI identified seven critical coverage issues:

1. Does the policy leave choice of counsel to you?

2. Does the policy cover system improvements required after a breach event?

3. Does the policy cover the replacement of systems after a breach event? (This is referred to as Bricking Coverage.) We may not think about it, but I actually had such a severe virus attack once that it disabled the server beyond repair and forced a replacement.

4. Does the policy cover business interruption coverage during the time it takes to get your computing environment restored?

5. What is the coverage sublimit, if any, for ransom or cyber extortion?

6. Does your policy provide for the high cost of crisis management and PR services?

7. Does your policy provide preventative pre-incident training?

I was not aware that a comprehensive cyber policy includes three distinct areas of coverage: first-party restoration, third-party protection and services for both prevention and to assist the firm if there is an actual event.

First-party coverage includes actual breach event costs like forensics and notifications, reputational harm, business interruption, ransomware/extortion, cyber-crime, bricking losses and property damage.

Third party coverage includes security and privacy liability, privacy regulatory defense and penalties, multimedia liability, PCI penalties and defense, bodily injury liability, pre-event training on risk updates, vendor best practices and employee training. Services also include post-event response, pre-approved experts and network recovery.

The last nugget I gleaned is about doing a risk analysis. After all, Rule 1.1 requires that you maintain competence:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

If you have never completed an application for cyber insurance, consider that doing so is a first step in conducting a risk analysis. Trust me, you will learn a lot about what risks you have not addressed simply by answering the application questions. I learned more about the "health" of my computing environment when I realized I didn't understand one of the application questions and had to turn to my IT team for guidance. It was eye-opening and helped me understand the scope of what I *didn't* know, which is always a good first step in risk analysis.

A version of this article originally appeared in the April 21, 2025 issue of Pennsylvania Bar News.

Freedman Consulting, Inc.
(215) 628-9422