ALPS Practice Management Pointers

Why You Want To Have Cyber Liability Insurance

Mark Bassingthwaighte, Esq.
mbass@alpsnet.com

An attorney's decision to use a computer tablet, a cloud based service such as Dropbox, a smart phone, a Wi-Fi network, or even basic email in the furtherance of delivering legal services is not in and of itself unethical nor a poor business decision. The real concern is with what the attorneys who use such tools do or don't do with them. For example, portable devices, which includes backup drives, can be lost or stolen; rogue programs that capture banking passwords, encrypt your data, or steal your data can be unintentionally downloaded; unauthorized access to your data can be achieved as a result of a successful phishing attack; and this list could go on and on. These kinds of breaches are often the result of common missteps such as lax security procedures, falling victim to a social engineering attack, and even simple ignorance about how a given device works or what a computer app or program really does.

You've read the headlines. Who hasn't heard about the Anthem breach, the NSA scandal, the Heart Bleed bug, Chinese cyber-spying, or the end of Windows XP support just for starters? And did you know that according to the 2012 ABA Legal Technology Survey, approximately 10 percent of participating law firms reported experiencing a data security breach of some kind? Taken together, one can surmise that cybercrime is going to continue to be a serious concern for the foreseeable future. Not be pessimistic but my personal perspective on the odds of a law firm having to deal with the fallout of a security breach is this. It's not if it will happen, it's solely a matter of when. Now if your response happens to be "we're too small to be on anyone's radar," please understand that a significant percentage of cybercrime attack vectors are automated. The size of the target isn't part of the equation. It's simply about taking as much data or money that can be taken.

A significant issue that must be addressed given the proliferation of cybercrime is what might the fallout be for any attorney or firm who experiences a data breach? The things that come immediately to mind include legal liability to others for the theft, loss, or unauthorized disclosure of personally identifiable non-public information; legal liability for the theft or loss of

third party corporate information; being subject to regulatory action or scrutiny due to the failure to comply with relevant security breach notification laws; having to cover the costs associated with responding to and recovering from the breach to include the costs of finding, notifying, and perhaps providing one year of credit monitoring for all who were impacted by the breach; the consequences of any loss or damage to your reputation; and the loss of revenue due to the breach.

Clearly technology is a double-edged sword. While its use by attorneys in order to practice is very appropriate, and I would argue mandatory in this day and age, doing so does expose attorneys to additional liabilities that can arise from identity theft, hacker malfeasance, cyber extortion, a security failure, hardware theft, and again, the list goes on. The problem is that for many there is an insurance gap in play. Should you ever find that your firm has been a victim of cybercrime would your existing insurance cover it? For far too many the answer would be no because malpractice policies and most general business insurance policies offer little to no coverage for cybercrime loses. The good news is that these risks can be properly covered with the purchase of a cyber liability insurance policy.

If you are not familiar with Cyber liability insurance products, know that they vary greatly in terms of cost and offered coverage provisions so a little comparison shopping might prove worthwhile. They are also claims-made policies which means that they must remain in force if one is to have on-going coverage. As a group these policies are designed to provide protection against things like the following:

Conduit Injury – a lawsuit resulting from a network security failure that caused additional damage to a client's computer network

Reputational Injury – a lawsuit resulting from an attorney's participation in social media

Disclosure Injury – a lawsuit resulting from the unauthorized access to or dissemination of client information

Content Injury – a lawsuit alleging intellectual property or copyright infringement perhaps due to postings on the firm's website or blog

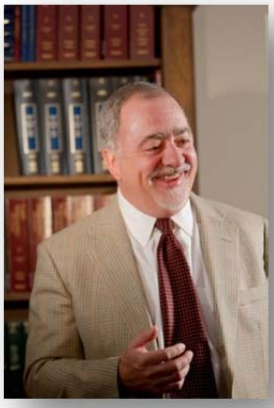
Privacy Notification Expenses – the costs associated with complying with relevant breach notification laws and with some policies can include the cost of attorney fees and/or credit-monitoring services

Crisis Management Expenses – the costs associated with bringing in outside experts to investigate the incident and fix the problem and with some policies can include the cost of a public relations consultant

Extortion Expenses – the costs associated with investigations or paying for the return of or gaining back access to data

Theft of Money – available with some polices but note that a separate crime policy may cover this as well

While one can never be completely free of the risk of becoming yet one more cybercrime statistic, the good news is that with the addition of cyber liability coverage this risk can be appropriately managed. Better yet, if you are an ALPS insured, this coverage is available as a separate policy on an opt-out basis which makes it quite easy to put a policy in place.



Risk Management Questions?

Mark Bassingthwaighte, Esq. is the Risk Manager for ALPS Property & Casualty Insurance Company. He is available to answer risk management questions and can be reached at 1-800-367-2577 or mbass@alpsnet.com.

Disclaimer:

ALPS presents this publication or document as general information only. While ALPS strives to provide accurate information, ALPS expressly disclaims any guarantee or assurance that this publication or document is complete or accurate. Therefore, in providing this publication or document, ALPS expressly disclaims any warranty of any kind, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Further, by making this publication or document available, ALPS is not rendering legal or other professional advice or services and this publication or document should not be relied upon as a substitute for such legal or other professional advice or services. ALPS warns that this publication or document should not be used or relied upon as a basis for any decision or action that may affect your professional practice, business or personal affairs. Instead, ALPS highly recommend that you consult an attorney or other professional before making any decisions regarding the subject matter of this publication or document. ALPS Corporation, as well as any of its subsidiaries, affiliates and related entities shall not be responsible for any loss or damage sustained by any person who uses or relies upon the publication or document presented herein.