USI Affinity Cyber Solutions For Law Firms

Not all data breaches are malicious cyber-attacks. A breach can be an employee error or even an internal system error. However, the consequences are the same and immediate response is required.

When it happens, are you prepared? Many law firms believe that cyber liability risks are already covered by legal professional liability (LPL) or indemnity insurance. While LPL insurance affords some coverage for cyber liability risks, there are limitations to the coverage provided by a law firm's LPL policy, and there are distinct advantages to shifting that coverage to a dedicated cyber policy.

As a leading specialty broker for law firms, USI Affinity's Cyber Practice has developed PrivaSafe, a proprietary cyber liability solution with NAS Insurance and a Lloyds of London syndicate. Our PrivaSafe cyber solutions product can offer law firms the comfort of knowing how to manage and mitigate exposures, and in the event of a data breach, they are protected.

For more information on the professional insurance products available to New York State Bar Association members, please contact:

Mike Mooney
Phone: 1.800.265.2876 ext. 1141
Email: Mike.Mooney@usiaffinity.com

For more information on Cyber Liability insurance please contact:

Greg Cooke
Phone: 1.610.537.1446
Email: Greg.Cooke@usiaffinity.com

www.nysba.org/NYSBACyber

NYSBA

We're with you at every step, elevating the practice of law with benefits that help grow your law practice.

Get to know your benefits at www.nysba.org/memberbenefits

NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, NY 12207
Phone 518.463.3200/800.582.2452
www.nysba.org
www.nysba.org/NYSBACyber

NEW YORK STATE BAR ASSOCIATION

A CYBERSECURITY GUIDE FOR ATTORNEYS

Learn how to protect your law firm's electronic assets. For more information, visit **www.nysba.org/NYSBACyber**.

Lawyers must keep abreast of the risks associated with managing technology and sensitive information, taking steps to safeguard themselves, their firm and their clients.

"[C]yber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. ***Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.***"

Committee on Professional Ethics, Opinion 1019 (August 6, 2014)
(emphasis added)

NYSBA

Protect yourself, your firm and your clients.

www.nysba.org/NYSBACyber

Protect firm computers and networks

Install security and antivirus software that protects against malware or malicious software on mobile devices and computers used within the firm or accessed from outside the office. Secure electronic communications as appropriate, through passwords or encryption, as well as the transmission of data stored in the cloud, ensuring secure "cloud" storage. Scrub "metadata" from electronic communications. Also, use a firewall program to prevent unauthorized access.

Require strong authentication

Ensure that users accessing your firm's network create strong user IDs and passwords/passcodes for computers, mobile devices and online accounts. Make sure users are accessing official websites when entering passwords/passcodes using a mix of upper and lower case letters, numbers, symbols and/or long, uncommon phrases. Differentiate passwords/passcodes on devices and/or accounts, changing them regularly in order to maintain passwords/passcodes in a secure manner. Be sure to never provide your passwords/passcodes to others.

Provide firm education

Establish security practices and policies for all firm employees. Monitor employees and enforce best practices pertaining to internet usage guidelines for mobile devices, internet usage, email and social media. Do not update software and apps unilaterally; instead, updates should be done after inquiry to the responsible individual or department. Identify an individual/department responsible for the above monitoring and advise all firm employees of the need to update devices upon consultation with appropriate personnel at the firm.

Access information on secure internet connections

Connect to the internet using only secure wireless network connections to ensure a private connection, such as a VPN. Public internet provided at airports, hotels and/or internet cafés may not be secure.

Suspicious emails, attachments and unverified apps/programs

Be suspicious of opening, forwarding or responding to unsolicited emails and attachments or links from unknown sources and be sure to charge phones on reliable USB ports. Do not download apps/programs from unverified sources to your computer or mobile devices, especially apps/programs that have access to contacts or other information on your mobile devices. Log out of apps/programs instead of simply closing the internet browser. And avoid file sharing services.

Software updates

Software vendors regularly provide patches and/or updates to their products to correct security flaws and improve functionality. Ensure timely patches and antivirus software updates are installed in all devices.