Cyber Liability for Law Firms

It is widely publicized that law firms continue to be growing targets for hackers and criminals in the cyber world. Much of the original discussion for purchasing and what was covered revolved around the amount of personally identifiable information (PII), personal health information (PHI) or personal credit information (PCI) that firms had. Given the values for this information (aside from PHI) have largely decreased on the black market, in terms of sale price, the confidential corporate information is much more valuable to the criminals. Law firms tend to have less sophisticated IT security than many other businesses, thus making them easy targets as we are beginning to see with some of the recent press for large and sophisticated firms. Also, employee error or theft remains one of the largest causes or breaches and firms must protect themselves from that element as well.

The first party costs associated with a breach are something that can easily get into the six figures. Coverages include the notification, forensic analysis to determine the cause of the loss, PR, business interruption, cyber extortion as well as regulatory fines and penalties. The regulatory piece is one that will continue to evolve in terms of dollar values. In fact the state of California requires businesses to use “reasonable security procedures and practices” when collecting or maintaining personal information and identifies minimum controls for this. Law firms do maintain a large amount of confidential corporate information that may relate to intellectual property, business transactions, mergers and acquisitions, information used against other parties in litigation and other information that should be protected by the law firm.

There are a number of carriers offering coverage in the market place for cyber liability, but the coverages differ and a firm’s broker should know what to look for. Some policies may only specifically cover personal information but don’t mention corporate information. Social engineering (when hackers deceive people so they give up confidential information or money) is one area the policy needs to be carefully scrutinized for. Also, does the policy have a carve-back for the employment practices liability exclusion so that coverage would apply if a firm’s own employee’s information is stolen? How does the “Other Insurance Provision” read? Finally, the coverage triggers for when the breach occurred are very important and policies look at them differently. Working with brokers that understand the policy forms and what is important for their clients is key in buying this coverage.

Cyber Security is an ever expanding area of risk across all businesses and must be looked at carefully. For small to mid-market firms who lack the IT infrastructure and financial resource of much larger firms the policy offers ancillary services as well as peace of mind. The ancillary services include pre-breach services with the ability to develop a response plan or look at areas the firm should focus on for development in IT security. Most importantly, every firm should ask themselves what they do when a breach occurs and how do they handle notification (it differs by state)? The best answer that can be arrived at is to let the professionals handle that and to purchase cyber liability through an experienced broker.

Nate Stortzum
Vice President
ProQuest, a division of Alliant Insurance Services, Inc.