5 Reasons Why **Law Firms** Need Cyber Insurance

1

CYBER CRIME

You may have already experienced phishing, telephone hacking, cyber threats, extortion, or unauthorized electronic funds transfer. These attacks are happening daily and law firms are a major target due to the sensitivity of the information they keep.

2

BUSINESS INTERRUPTION

Law firms are increasingly reliant on their computer systems to provide services, conduct business, and to communicate with clients and other third parties. As a result, law firms could suffer significant loss of revenue in the event of an interruption of their networks or systems.

3

REPUTATIONAL HARM

Law firms rely heavily on their reputation to attract potential clients. A data breach can shatter current and future client's perceptions of the firm. Client's need to feel that their confidential information is secure.

4

PRIVACY LIABILITY

Every day, your Law Firm stores and transfers large amounts of electronic information. Personal client information and vital internal information is stored on your systems. If you have a security breach and this information is exposed, the cost of a third party lawsuit can be staggering.

5

NOTIFICATION COSTS

If you lose sensitive data you have a legal duty to your clients. They have a right to know if their confidential information is available to the public. You may have only a few clients or you may have thousands of clients. Once they are notified there is a higher chance of a suit.

"There are two types of companies: those who have been hacked and those that will be."

Robert Mueller, FBI Director 2012

CLAIMS EXAMPLES

A law firm insured received a call from a defense contractor who reported it had been tracking hacking activity related to a particular domain name. The contractor reported that it had detected evidence that IP addresses associated with the law firm's computers were purportedly communicating with the suspicious domain name. The firm retained a forensic investigator to assist with the investigation and legal counsel to provide legal advice with respect to the breach. These services cost between $400,000 to $600,000 and were covered by the firm's cyber policy.

Immediately prior to his departure from an insured law firm, an associate who had resigned by email wiped out all of the hard drives available to him and removed the firm's intellectual property and proprietary information from storage devices and backup systems. The insurance company's cyber security response team worked closely with the law firm to recreate all of the applications and information that had been erased, a process that took about 1,100 man-hours to complete. The law firm was reimbursed approximately $300,000 in costs.

Approximately 100 attorneys and staff members were Bcc'd on a phishing email attaching a file which appeared to be attorney-client work product. When each user attempted to open the attachment, the user was prompted to enter his or her Outlook username and password. Over the next 20 hours, the intruder entered the firm's Outlook server and accessed several hundred email messages. The firm retained a forensic consultant and law firm and the matter was resolved within the firm's retention.

COST ANALYSIS

What does it cost your business when 100,000 records are breached?