Why Law Firms Need Cyber Insurance

Law firms are increasingly falling victim to cyber attacks. Due to the wealth of confidential information inherent in the industry, **law firms make attractive targets to hackers.**

The variety of material vulnerable to a breach ranges widely by firms' specialties. These include:

- Employee and client personally identifiable information (PII)
- Sensitive contract documents
- Private corporate data
- Criminal activity records

Shielding firms from the costs of a breach or a ransomware attack requires comprehensive cyber coverage. Ransomware attacks are especially difficult for law firms when the data is exfiltrated where the hackers will then threaten to release the confidential data into the public domain if they don't pay, possibly ruining the law firm's reputation. So even if the law firm had good enough controls to recover from the event, they may still have to pay.

The Cost of a Breach

Breaches **often cost millions of dollars.** For the largest firms, this amount could be a weatherable hit. But for small- and mid-sized firms, the expense of a cyber attack could likely spell bankruptcy.

Aside from its direct costs, a successful cyber attack on a firm can also have a number of indirect, **deeply damaging effects**. These could include:

- Lost revenue from an interruption of daily activities
- Legal fees and payments from malpractice suits related to the hack
- Reputational damage affecting business down the line

Fortunately, all these damages can be covered or mitigated under a cyber insurance plan.

Implementing Cyber Security Controls

Due to the constantly growing risk associated with providing cyber insurance, most carriers will not offer coverage without such basic cybersecurity precautions in place as:

- **Multi-factor authentication** (requiring more than a name and password for access)
- **Endpoint protection** (monitoring and scanning of servers and devices connected to the network)
- **Secure email gateways** (weeding potentially malicious messages out of incoming email)
- **3-2-1 backups** (three copies of data, two local but on different devices, one off-site)

What Does Cyber Insurance Cover?

First-Party Coverage

- Hiring forensic IT consultants to determine the origin of the breach
- Outsourcing support to manage impacted clients
- Repairing digital assets and replacing equipment
- Following state-specific reporting guidelines

Third-Party Coverage

- Legal representation
- Document preparation
- Regulatory fines
- Payouts to affected customers

A Real World Example

In early 2021, a sophisticated phishing scheme targeted 48 top Chicago law firms. The hacker, operating out of Ukraine and going by the name Oleras, was looking to gain access to mergers and acquisitions information in order to conduct insider trading. In the last few years, corporate law firms have become a target for hackers as a sort of “back door” into the financial sector. As of this writing, no evidence of hackers successfully leveraging the stolen information exists, but such a hack could carry serious financial and reputational repercussions for a firm.

Data breaches can affect anyone. The stakes are too high for law firms to go unprotected. Get cyber insurance today.