Cyber Risks: Liability Protections for Legal Professionals

Law offices handle a considerable amount of sensitive data related to their clients and cases, making them a potential target for various cyber threats. With cyber crime on the rise, legal professionals face substantial risks from regulatory, financial, and reputational perspectives.

In our guide below, we'll present common cyber threats, then provide mitigation strategies that supplement the protections afforded by cyber liability insurance.

To learn more about lawyers' professional liability, including cyber insurance options, visit the USI Affinity Insurance Solutions page at https://www.usiaffinity.com/attorneyspreferred/lpl/.

Common Cyber Threats

Sensitive data collected, shared, and transmitted from legal offices to courts and insurers represents a tantalizing target to criminals. Cyber criminals may sell this information, hold it hostage, or alter it for their own purposes. With the average cost of a data breach exceeding $4 million per incident, law firms face staggering financial concerns, not to mention the reputational damage a data breach can cause.

Common cyber threats challenging law firms include:

Data breaches: unauthorized access or theft of confidential legal data, including personally-identifying information (PII).

Ransomware attacks: data is held hostage by criminals who encrypt the information and demand payment to restore access to it.

Phishing attacks: from deceptive emails and fraudulent website redirects to downloading malware onto office computers, criminals using phishing attacks can gain access to data and computer systems.

Physical theft or loss: criminals stealing work laptops and mobile devices may gain access to client data and computer systems, potentially leading to severe financial and regulatory repercussions.

Software/network vulnerabilities: outdated antivirus/anti-malware software or inadequate network security may provide "backdoor" entrances for criminals to steal or destroy sensitive client data.

Criminals have become more sophisticated in recent years, using social engineering hacks and software vulnerabilities to copy, steal, or erase data. With this looming threat over the legal profession, it is imperative that law offices take the steps needed to protect client information from loss.

Cyber Risk Mitigation for Legal Practices

Now that we've learned about the potential threats – and the strategies criminals use to gain access to sensitive legal data – what are risk mitigation strategies that law offices can use to protect this data?

Risk management for cyber security is a multi-pronged approach that includes policy, training, and incident management components. This approach may include:

. Technological Measures:

- Utilize firewalls, antivirus software, and data encryption.
- Employ multi-factor authentication and secure wireless networks.
- Ensure regular data backups.

2. Policy and Compliance:

- Establish a thorough cybersecurity policy.
- Adhere to all applicable cybersecurity regulations.
- Include cybersecurity aspects in client and vendor contracts.

3. Training and Culture:

- Implement ongoing cybersecurity training for staff.
- Promote a general awareness of cybersecurity risks and practices.

4. Incident Management:

- Develop an incident response plan and define breach notification protocols.

5. Device and Network Management:

- Implement network monitoring and secure device management policies.

6. Vendor Security:

- Manage vendor cybersecurity through evaluations and secure communications.

7. Physical Safeguards:

- Control physical access to facilities and secure hardware components.

8. Cybersecurity Audits:

- Conduct periodic cybersecurity audits and vulnerability assessments.

Ensuring a blend of technological security, policy adherence, staff training, and robust incident response, along with consistent audits, will form a strong cybersecurity posture for law offices.

Of course, cyber liability insurance is the foundation upon which risk management is built. Cyber liability solutions typically include first- and third-party coverage against the costs associated with data breaches, data recovery, reputation repair, and crisis management after a breach or data loss has occurred.

Selecting the right cyber liability insurance program involves evaluating the specific risks and exposures of the business and ensuring that the policy's coverages adequately address them. Working with an experienced insurance broker or advisor, and carefully reading policy documents, can assist businesses in procuring optimal cyber insurance coverage.