PREVALENT®

Need to Know:

Law Firms & Third-Party Risk

THE TOP 5 THINGS YOU NEED TO KNOW ABOUT MANAGING VENDOR RISK TO PROTECT YOUR CLIENTS' DATA AND PRIVACY

Law firms handle some of the most sensitive and private information, yet many haven't taken the necessary security steps to protect themselves or the private data of their clients. Fueled by a dramatic rise in vendor outsourcing, along with the expansion of digital business, both regulators and managing partners see the threats arising from the actions of third parties as real and worrisome. Here's what you need to know about the importance of developing and maintaining a scalable third-party risk management program to meet the regulatory requirements of your clients, while ensuring the security of your own intellectual property and private employee information.

1 It's your responsibility to manage vendor IT security, data and privacy risks

It often makes good business sense to focus on core competencies and outsource any functions that can be operated more efficiently by other companies. So while your clients are concerned with how well you manage IT and data security, they also need assurance that you require your vendors to provide the same levels of protection. **Remember, just because you outsource to a third party, it doesn't mean you outsource the risk.** A data breach at one of your vendors that involves your client's data is your responsibility and directly impacts your relationship with all of your clients.

2 Clients expect your third-party risk management program to be as robust as theirs

Clients expect that their law firms' third-party risk management programs will mirror their own, due to the ever-expanding regulatory requirements requiring them to be aware of how their vendors manage risk. **Therefore, it is extremely important to understand the regulatory requirements placed on your clients and their expectations for how you will manage your own vendors.** Achieving proper visibility and monitoring of your vendors' compliance with security regulations and best practices is required by many regulatory and security guidelines, including PCI DSS, OCC, HIPAA, 23 NYCRR 500, NIST, and ISO, just to name a few. Law firms should also be concerned with data privacy legislation, such as GDPR and CCPA.

3 Your firm is an extremely attractive target for criminals

Many of your client relationships require you to have access to your clients' customer data, their systems, and intellectual property. This makes you a very attractive target for criminal activity. **Cyber criminals look for the weakest link in the supply chain and have developed sophisticated attack tools and techniques to gain access to valuable PII.** You may continue to improve your security posture and build up perimeter defenses, but if the same cannot be said for your vendors, then you are putting your clients' data, and your reputation, at risk.

4 Many regulations and industry frameworks require both internal assessment and external monitoring

With no vendor attestation, scoring and ratings provide a limited external view of vendor risk; they do nothing to determine what controls are in place, or what IT security and data privacy policies and procedures a vendor follows. Telling half the story doesn't meet regulatory guidelines either. **Several state and federal regulations, as well as industry frameworks, require a complete inside-out and outside-in view of risk from a combination of vendor questionnaires and continuous monitoring.** Your clients can't afford for you to be out of compliance.

5 Third-party risk management is costly without an automated, standards-based approach

Manually performing the vendor assessment process requires substantial time and resources. Sure, a manual approach may be fine for one vendor, but what if you have business relationships with hundreds or thousands of third parties? **Spreadsheets, emails, and haphazard data-sharing efforts give rise to inefficient, error-prone processes and are not scalable.** Moreover, different assessments must be developed for each type of outsourced service. Each vendor must go through a scoping process to ensure that the appropriate assessment is used to evaluate proper risk controls. Then, the results of these questionnaire must be fully analyzed and remediated. Managing the risk posed by third parties needs to be automated and standards-based.

The Legal Industry's Preferred Third-Party Risk Management Platform

Prevalent's Legal Vendor Network delivers an efficient, scalable third-party risk management platform to satisfy client compliance requirements and reduce risk. Prevalent is the only third-party risk management provider that unites deep controls-based internal assessments with external scanning for a complete, 360-degree view of vendor risks.

Key Benefits

Massive time and cost savings
Typically, more than 40% of a firm's vendors are already in the Network, meaning the assessments are already done!

Immediate line of sight into risk
Gain instant access to vendor data survey and monitoring intelligence.

Greater efficiency
Eliminate manual tracking and spreadsheets with an automated, standards-based approach.

Meets auditor demands
Demonstrate compliance with contractual or regulatory obligations with stakeholder-specific reporting.

Strong data control practices
Protect against cyber-attacks and data breaches.

Join nearly half of the top 100 U.S. law firms in Prevalent's Legal Vendor Network. Contact us today!