Vendor and Third–Party Cyber Risk: Your Weakest Link May Not Be Inside the Firm

When cybersecurity researchers analyze how law firm breaches actually happen, a consistent finding emerges: In a significant percentage of cases, the initial point of compromise wasn't inside the firm at all — it was a vendor.

The Vendor Problem in Law Firm Cybersecurity

Modern law firms depend on a large and growing ecosystem of third-party technology vendors: cloud-based document management systems, e-discovery platforms, managed IT service providers, legal research tools, billing and practice management software, and client-facing portals. Each of these vendors has access to firm systems, firm data or both.

The security posture of those vendors varies considerably. A large, well-resourced e-discovery company may have enterprise-grade security controls. A boutique managed IT provider serving small to midsize firms may not. And the firm's cyber policy, the firm's security team, and the firm's management committee may have little visibility into which vendors represent real risk and which don't.

What a Third-Party Breach Means for Your Coverage

When a breach originates through a vendor, the coverage picture is more complicated than a direct attack on the firm. Most cyber policies provide some coverage for losses resulting from a vendor breach, but the specifics matter enormously.

Key questions to ask about your current policy: Does your policy define covered vendors broadly or only those listed on a schedule? Does business interruption coverage apply when a vendor's outage disrupts your operations even if your own systems are uncompromised? Does your policy require you to notify the insurer when a vendor reports a breach that may have exposed your data, and how quickly? Firms that don't understand the vendor-related provisions in their cyber policy may find themselves underinsured when a third-party breach affects their operations or client data.

Building a Vendor Risk Management Program

You don't need to build a sophisticated vendor risk management program overnight, but you do need a baseline. Start by inventorying the vendors that have access to firm systems or client data. Prioritize them by the sensitivity of data they can access. For high-priority vendors, request evidence of their own cyber insurance, review their security certifications, and confirm that your contract includes appropriate data security and breach notification requirements.

Vendor contracts should require prompt notification of any security incident that may have affected your data, rather than notification at the vendor's discretion. This should be a defined window that allows you to comply with your own policy's reporting requirements. Many firms discover that their vendor contracts say nothing about cybersecurity obligations at all, which is itself a negotiating point worth addressing at renewal.

A Word From Gallagher

Gallagher works with law firms to assess how their cyber coverage responds to third-party breach scenarios and to identify gaps before a claim surfaces. We can also help you think through vendor contract requirements from an insurance perspective. Contact our law firm practice team to learn more.

Connect with us

ANDREW HAUGEN
M: (516) 434-9407
E: andrew_haugen@ajg.com

Want more information about our Law Firm expertise?

www.ajg.com/NELawfirms