Cyber Extortion Is No Longer an IT Problem ... It's a Firm Leadership Problem

The average cost of a ransomware attack on a professional services firm now exceeds $1.5 million when you factor in downtime, recovery, legal notification costs and reputational damage. And law firms are among the most targeted organizations in the country.

Why Law Firms Are Prime Targets

Law firms hold extraordinary concentrations of sensitive data: M&A deal terms before public announcement, litigation strategy and privileged communications, personal financial information for high-net-worth clients, and protected health information in healthcare or personal injury practices. To a ransomware operator, that data isn't just valuable, it's doubly valuable, because firms face both the cost of recovering their systems and the threat of having client data published publicly if they don't pay.

This dual-extortion model (encrypt your systems and threaten to publish the data) has become the dominant ransomware playbook. And it's particularly effective against law firms because client confidentiality isn't just an ethical obligation; it's a business relationship built on trust. The pressure to pay can be significant.

The First 24 Hours Define the Outcome

Law firms that have been through a ransomware event will tell you the same thing: what happens in the first 24 hours matters more than almost anything else. Firms that respond well have typically done one thing differently, they've planned for it in advance.

A cyber incident response plan should establish clear decision-making authority before an event occurs. Who makes the call to take systems offline? Who contacts outside counsel? Who engages the incident response team? Who communicates with clients? Without those answers written down, firms make worse decisions under pressure and lose critical time.

Most cyber insurance policies include access to a panel of preapproved incident response vendors such as forensic firms, ransom negotiators, legal counsel and PR support, but only if you notify your insurer promptly. A 48-hour delay in notification can complicate your claim and limit your options.

What Your Cyber Policy Actually Covers and What It Doesn't

Cyber insurance policies have evolved significantly, but there is still meaningful variation in what different policies cover. First-party coverages typically include costs to restore or recreate data, business interruption losses during system downtime, ransom payments (where legally permissible) and the cost of forensic investigation. Third-party coverages address liability to clients whose data was compromised, regulatory defense costs and notification expenses.

Where firms often get surprised: sublimits on specific coverages (ransomware payments, business interruption and funds transfer fraud are commonly sublimited), waiting periods before business interruption coverage kicks in, and exclusions for unpatched systems or failure to maintain basic security hygiene like multifactor authentication. Understanding these terms before a claim is far better than discovering them during one.

A Word From Gallagher

Gallagher works with law firms to review cyber policy terms, identify gaps between coverage and actual exposure, and help firms build the incident response infrastructure that carriers increasingly require. If your firm hasn't conducted a cyber coverage review in the past 12 months or hasn't tested your incident response plan, we can help. Reach out to our law firm practice team.

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