CYBERSECURITY AWARENESS CAN KEEP SMALL AND MID-SIZED LAW FIRMS IN THE BLACK WHILE AVOIDING A BLACK EYE

THE ABA MODEL RULES APPLY TO CYBERSECURITY

When the ABA approved a change to its Model Rules of Professional Conduct, it reemphasized the perils and promises of technology.

EMPLOYEE ACTIVITY APPLIES TO THE FIRM

Even a lack of proper employee supervision could be characterized as negligent and rise to the level of fraud and misrepresentation if caused by a malicious or ignorant insider.

THEIR DATA IS YOUR DATA

Law firms must treat data from their clients with the same level of protection as if they were the original owners.

LAW FIRMS ARE TARGETS

Law firms are targets because they have highly-valued material with weaker safeguards to protect sensitive data.

PARTNERS
IN REGULATORY COMPLIANCE

DATA PROTECTION MATTERS IN MALPRACTICE

Insufficient data protection could result in malpractice claims for failure to preserve client confidentiality.

INSURANCE IS NOT ENOUGH

Even firms that have cybersecurity insurance cannot afford to lose the lifetime value of an institutional client or the potential to gain another due to a loss of standing in the legal community.

POLICIES AND REPORTING PROTOCOLS ARE PARAMOUNT

Organizations with proper policies and adequate reporting structures are often able to address security concerns more quickly and effectively.

LOST DATA LEADS TO LIABILITY

If a law firm's data ends up on the “dark web” and a client's information is sold or released as a result, the liability could be substantial. The firm would also be negatively impacted and could potentially suffer reputational or operational damage.

Partners in Regulatory Compliance provides an array of cybersecurity services, including policy creation and management, risk assessments, employee training, and regulatory compliance assistance to law firms in New York, New Jersey, and Connecticut.
Contact us at (646) 863-9050 or info@piregcompliance.com.