CASE STUDY

Upholding Lawyer-Client Privilege

Corporate law firms make attractive targets for ransomware and other cyberattacks because they have vast amounts of confidential information about their clients. Lawyers themselves have proved susceptible to phishing attacks and are thus high-value targets in an industry where brand reputation is everything.

Yet many top firms aren't in the position to invest the money needed to build an effective in-house cybersecurity team. As a result, even firms with thousands of lawyers across dozens of international offices, most including Fortune 100 clients, lack the appropriate protocols to adequately protect client data.

Trustwave®
Smart security on demand

CLIENT SPOTLIGHT

A top AmLaw100 firm with nearly 2,000 lawyers across dozens of offices worldwide that serves more than half of the Fortune 100 companies.

THE CHALLENGE

This AmLaw100 firm was feeling the heat as cybersecurity challenges mounted. Not only was it struggling to retain its understaffed in-house security team and failing to recruit new members in a wildly competitive job market, but the overwhelmed staff wasn't able to properly implement and maintain the expensive technology tools the firm had purchased to improve security.

At the same time, the firm's partners were watching devastating breaches occur in the industry with increasing frequency. In 2016, the Wall Street Journal reported that a ring of insider trading cybercriminals compromised files from some of the country's preeminent firms, searching for not-yet-public information about clients and forthcoming deals. That same year, a law firm was hacked and troves of sensitive files about its high-profile clients' offshore tax secrets flooded the media. With client relationships at stake, the firm understood the urgency of engaging a trusted third-party expert who could manage the firm's already-strong security technology and create a world-class security center that matched its world-class legal reputation.

> *"Cybersecurity is challenging enough without another vendor telling you what to do. Trustwave was unique in seeking first to understand our industry and environment, then partnering with us to customize the best possible service plan to achieve our security objectives. It was a true partnership from the beginning and my team can now focus on adding more security Plan and Build value while they manage the Run."*
>
> – CISO AmLaw100 Firm

THE SOLUTION

Given the small size of its in-house security staff, the firm decided to fully outsource to Trustwave the management of its enterprise security information and event management (SIEM) solution, its intrusion detection and prevention systems and its next-generation firewalls. The firm also engaged Trustwave to consult on its vulnerability management, detection and response program and to serve as its information security advisor. With Trustwave's staff acting as an extension of the in-house security team, the law firm was able to increase its security operations' productivity by a whopping 57 percent. The firm was able to extend security coverage, quality and reliability at a fraction of the cost of providing these services internally.

With Trustwave's Global Threat Operations specialists, they scaled their cybersecurity team three-fold providing 24/7 coverage with certified experts who are organized to respond to security incidents and remedy security problems. With a more stable day-to-day system in place, the firm's IT team was able to take the time to perform a broader risk assessment with Trustwave and create a roadmap for its future security plans.

INDUSTRY THREAT

Attacks on law firms are increasing as hackers seek to steal client information or extort money from firms via ransomware. Phishing attacks remain popular as well, given the large number of users at a big firm. And as firms shift to cloud-based systems for around-the-clock client communication, more potential data loss scenarios emerge.

Despite the potentially catastrophic nature of a breach, many law firms still risk being caught flat-footed. According to the 2017 American Bar Association technology survey, only 26 percent of all firms report having an incident response plan in place.

The upside to that disquieting figure is that any firm presenting a unified, top-tier cybersecurity protocol will stand out.

Trustwave®

Smart security on demand

CS-LAW-0418