To Improve Law Firm Cybersecurity, Innovative Computing Systems Partners with Digital Defense

Through the partnership, Innovative Computing Systems and Digital Defense aim to improve law firm cybersecurity technologies and best practices.

Ian Lopez, Legaltech News

June 27, 2016

With both high and low profile breaches making news in recent years, cybersecurity is a front-of-mind issue for law firms. Among the companies looking to help lawyers protect the valuable information hackers increasingly seek is law firm tech-provider Innovative Computing Systems, which today announced a partnership with data protection company Digital Defense, Inc. (DDI) to help law firms defend against cyberattacks.

Through the partnership, experts from both companies will assist law firms in beefing up their cybersecurity infrastructure via best practices, "awareness education," and "regular

SECTIONS

Product News and Reviews
Cybersecurity
Law Firm Management
Legal Operations

More From Legaltech News

What's on the Frontier in Legal Tech?

Ready or Not, Lawyers are Increasingly Bound to AI by Ethical, Legal Standards

Law Firm CIOs and Directors Provide Perspective on Evolution of Legal Tech

Confronting Negligence and Insider Threats, Lawyers' Cybersecurity Efforts Usually Begin Post-Breach

assessments," Innovative noted in a statement announcing the partnership. Company CEO Michael Kemps added in a statement that the goal of the partnership is "to bring the latest best-in-breed cybersecurity solutions to law firms," and defend against a variety of attacks, including whaling and phising.

Kemps told Legaltech News that through the partnership, the companies can scan client networks "for vulnerabilities" in an effort to ensure threats are "locked down and eliminated." He added that currently, law firms are increasingly being audited by clients because of data breaches, and scanning firms for security threats "provides law firms and their clients with confidence."

"Law firms are facing cybersecurity issues from all fronts," Kemps explained. "Their end users do not make adequate time for security training, nor are they sufficiently careful with opening attachments that may be laden with ransomware. Professional services firms historically 'set it and forget it' when implementing technology. This creates massive risk. Environments are frequently not patched and kept current. This increases vulnerability exponentially."

As to how this partnership allows Innovative and DDI to approach cyberthreats, Kemps noted that the companies look at cybersecurity as a "multilayered discipline," and that "engaging a third-party specialist to ethically and reliably scan and identify potential issues is in the best interest of all parties and positions us all for success."

"The days of simply depending on a firewall and anti-virus software are gone. Intrusion detection, unified threat management, advanced end point protection, two-factor authentication and mobile device management and training are all areas of focus that law firms have generally overlooked," he said. "Going forward, firms will continue being audited by the clients; their use of technology and cybersecurity will be reviewed and validated. Hitting the ground running by turning security into a managed service is not only proactive, it's now required."

Data breaches are increasingly a problem for law firms. According to the 2015 American Bar Association Legal Technology Report, 15 percent of responding law firms experienced a data breach in 2015, up from 14 percent in 2014. About 42 percent of respondents reported that their firm was infected with virus/spyware/malware, while 30 percent noted that a breach resulted in downtime/loss of billable hours.

The report also found that 47 percent of firms didn't have an incidence response plan to handle a data breach, while 25 percent of respondents didn't know whether their firm had one.

As to how law firms can bolster their on cybersecurity, Kemps advised they start "hardening their environments: implementing password complexity; employing two-factor authentication; utilizing mobile device management tools; and by keeping servers, workstations and networking equipment updated and patched; and, lastly, with better educating the user population to both understand the risks and be cognizant of the exploits." However, he added that, "All of these approaches depend on an environment that is properly architected."

"We see law firms continuing to face increasing risk. Those that address the subject aggressively will be protected. A continued lackluster approach to management, oversight and use will expose firms to potential data loss, opportunity cost and the destruction of reputation, leading clients to question relationships," he added.

Related Articles:

- Tech Companies Face Mixed Impact from Brexit Vote
- Meeting Ransomware Threats with SIEM
- Law Firms Increasingly Joining Information Sharing Centers for Cyber Threat Info