Angie Hickey Featured in ABA Discussion on Law Firm Data Security

April 19, 2016

Executive Director Angie Hickey shared valuable insight in the American Bar Association's roundtable discussion addressing law firm data security.

The revelation that some of the country's most prestigious law firms were hacked in an attempt to uncover confidential information, coupled with the "Panama Papers" scandal, has put an uncomfortable spotlight on law firms and their data security programs.

This may be the much needed wake-up call to law firms-big and small-to conduct an audit of their information security systems and protocols, and be more proactive in their efforts to prevent data breaches that could potentially have significant ramifications, both for their clients and their livelihood.

In this month's roundtable, law firm leaders and cybersecurity experts discuss why law firms are vulnerable to hackers, and what needs to be done to prevent a consequential data breach. Angie's responses are featured below.

What was your response to the revelation that recently a number of law firms had been hacked?

" *This is not surprising. Law firms possess highly sensitive and confidential information and also have access to large amounts of money.*"

How seriously do most firms take the issue of data security?

" *This is a very significant concern for law firms of all sizes. Law firms are held to a strict standard and have a duty to protect the confidentiality of clients and client information.*"

What can/should the typical law firm do-that it is not currently doing-to better protect client information?

" *It is standard industry practice to request all employees to annually sign confidentiality agreements and also to require non-disclosure agreements from all external vendors. It is also standard for law firm technology infrastructure to include security monitoring systems, firewalls, blocking the ability to upload files to external devices, frequent password changes, etc. Our firm also has regularly scheduled penetration tests as*

part of an annual security audit performed by an outside technology company. Despite every recommended precaution, the largest risk of a cyber breach is through the people who work in law firm. It is important to find ways to heighten the awareness levels and to train law firm employees on their role in preventing cyber breaches."

Do you think clients are aware of the risk they run when sharing confidential information with lawyers?

" *Unless they have worked in a law firm, I don't think clients know "how the sausage is made" and many would probably be surprised at how fluid information-sharing is within a law firm. Clients should ask to see a firm's business continuity plan, or at the very least have a conversation with their law firm about the precautions in place to guard against the risk of a cyber breach.*"

What does the future hold for law firm data security?

" *More layers of security for access to information. It's interesting to consider that many law firms have responded to client pressure for cost reduction by outsourcing seemingly low level tasks such as document review and production. Outsourcing and offshoring arrangements may lower the*

personnel cost of a law firm but they also increase risk and may just shift the cost to other areas, namely IT and security. It is also interesting to consider that as clients demand faster response times, law firms may actually need to slow things down in order to reduce risk of cyber breach. This can be frustrating for clients and also adversely impact outcomes because so many transactions are time sensitive."

To read the full article and other featured responses, please follow the links below.

Law Firm Data Hack Attack, Part I
Law Firm Data Hack Attack, Part II