Guidepost

ARE LAW FIRMS IN THE CYBER CRIMINAL'S CROSS HAIRS?

From the Panama Papers to the recent indictment of three Chinese nationals for insider trading using stolen M&A information, law firms have become a target for information theft. In many cases, the targeted law firm represents clients that have made significant investments in their own cyber security, and adversaries recognize that their attorney's networks are often a much softer target. In addition to the cyber attacks in the news headlines, there are an increasing number of breaches occurring that are not publicly disclosed.

Increasingly, more law firms are protecting themselves as they would their clients.
Law firms are data managers just like any other business enterprise. They have data concerning their own employees, their clients and their clients' business activities. All that data sits in a digital network for which the necessary tools of practice – smartphones, remote log-in, portable devices, etc. – unavoidably create risk. Moreover, law firms which service clients in regulated environments, such as financial entities and health care providers, are inevitably finding themselves bound by the same regulatory scheme as their clients.

For example, the New York State Department of Financial Services has issued cyber security regulations for regulated entities and third-party providers (23 NYCRR 500). Regulated entities must, by March 2019, ensure that all third-party vendors who hold any confidential data of a regulated entity must be compliant with certain provisions of the regulations. In addition, HIPAA regulations similarly require that all business associates of regulated entities comply with its privacy and security provisions. Neither set of regulations carves out an exception for law firms from being considered as a vendor or business associate.

And, the pressure keeps building. On March 29, the Association of Corporate Counsel issued its Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information ("the Model"), describing it as "a benchmark for law firm cybersecurity practices." To describe the guidelines as demanding would be an understatement. Beginning with a definition of "Company Confidential Information" that includes a broad range of client data and information, the Model addresses data retention, data handling and disposition, encryption, data breaches, physical security, access controls, network monitoring and security, risk assessments, the right of the client to review the data security practices of the law firm, background checks on law firm personnel who come in contact

with client data, cyber insurance and incorporation of the Model into any contracts with vendors providing services related to the client data. This is clearly a clarion call for all law firms to take their cyber security practices seriously.

Of course, the cyber security wake up call for law firms has been ringing for some time. A recent indictment exposed the scheme of foreign nationals who penetrated the computer systems of multiple law firms to steal insider information to guide their investments. According to the indictment, the defendants spent months inside the law firms' networks stealing information. The massive disclosure of confidential client information commonly known as the Panama Papers underscores how a law firm's ethical obligation to protect client confidentiality has evolved in the internet era.

Moreover, at a very practical level, beyond issues of confidentiality and embarrassing headlines, efforts to mandate cyber security for law firms are becoming thresholds for being able to do business. Law is a competitive industry. One firm's ability to market and demonstrate its compliance with the principles of cyber security can provide it with a distinct competitive advantage over other firms which may be able to offer identical legal services. Failure to achieve compliance could leave a firm as obsolete as if it were still using typewriter ribbons and whiteout.

JOHN TORRES

President, Security + Technology Consulting

John P. Torres is the president of the Security & Technology Consulting practice for Guidepost Solutions. John has extensive investigative and security experience. Previously, he served as the Special Agent in Charge for Homeland Security Investigations in Washington, D.C. and Virginia. His background includes more than 27 years of experience providing investigative and security management for the U.S. Departments of Homeland Security and Justice, including serving as the Acting Director and the Deputy Director of U.S. Immigration and Customs Enforcement.

KENNETH CITARELLA JD, MBA, CFE, CIPP/US

Senior Managing Director, Investigations and Cyber Forensics

Ken Citarella guides the international compliance efforts of the firm in its investigative, security consulting, due diligence and compliance consulting practices, including advising clients on how to create and maintain a privacy compliance program. An attorney and Certified Information Privacy Professional by the International Association of Privacy

Professionals, Mr. Citarella was one of the earliest prosecutors in the nation involved in the investigation and prosecution of computer-based crime. The High Technology Crime Investigation Association bestowed its Lifetime Achievement Award on Mr. Citarella in 2011.