Recent Cyber Attack On Law Firms Serves As A Wake-Up Call For Professional Services Firms

Cyber criminals are becoming more sophisticated and are expanding their targets to include professional services firms that possess confidential information as illustrated by recent highly publicized cyberattacks on law firms. Data breaches not only bring unwanted media attention, but also raise concerns among clients about how vulnerable their data is in the hands of service providers. Consequently, professional services firms should continuously assess their cyber-risk exposures.

THE RECENT CYBERATTACK ON LAW FIRMS

On December 25, 2016, the U.S. Attorney for the Southern District of New York filed criminal charges against three Chinese individuals for having implemented a sophisticated scheme to trade on insider information about unannounced upcoming corporate transactions involving publicly traded companies[1].

The scheme involved gaining access to the email servers of at least two prominent New York law firms through the use of malware. Once inside the firms' systems, the hackers stole copious amounts of data from the emails of several partners, containing details of unannounced M&A deals. Armed with this confidential information, the defendants traded in the stock of the companies involved and racked up at least $4 million in illicit trading profits. The transactions at the heart of the allegations include notable acquisitions involving Intel, Pitney Bowes and others.

The breach involved in this case will not be the last time the computer networks of professional services firms, large and small alike, are exploited by domestic or international criminals, as the legal industry has already learned with such stories as the "Panama Papers" breach in early 2016.

CONSEQUENCES

It should not surprise accountants, investment bankers, lawyers and other professionals that they are prime targets for cyber criminals. This is especially true for those who are involved in transactions the details of which are easily monetized, such as through illegal trading. Nevertheless, cybersecurity practices at professional services firms tend to be weak. The consequences of a data breach for professional services firms can be devastating, in terms of the damage a breach can cause to their clients' businesses, and the reputational and public relations impact on the firm itself. For example, a professional services firm that has suffered a data breach may face potential legal liability to its clients, and may have violated applicable ethical rules. A class action complaint recently unsealed in Illinois accuses Chicago-based law firm Johnson & Bell of inadequate security protections for client data, even though there is no allegation that any data was actually stolen.

Additionally, as the U.S. legal and regulatory landscape evolves, professionals might find that they have violated a variety of federal and state statutes, that require businesses to exercise due care in protecting their clients' private data from cyberattacks.

[1] The U.S. Department of Justice's press release is available at https://www.justice.gov/opa/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against-three.

EMERGING CYBERSECURITY STANDARDS

Consequently it is becoming increasingly clear that law firms, accounting firms and other professional services firms can no longer wait to assess and address the cyber risks they face. Professional services firms should implement measures, both institutionally and technologically, to mitigate these risks. Best practices are beginning to emerge, including those enunciated by the Center for Internet Security, and the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework. The California Attorney General has said that "the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." Every professional firm needs to review and implement those controls.

For more information on the topic discussed, contact **Andre R. Jaglom** at **jaglom@thsh.com, David R. Lallouz** at **lallouz@thsh.com**, **Michael Riela** at **riela@thsh.com,** or any other member of the Firm's Cybersecurity and Data Privacy Practice. For more information on Tannenbaum Helpern's Cybersecurity and Data Practice's capabilities, visit us at **www.thsh.com**.