Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Panama Papers: Reminders About Law Firm Cybersecurity

Law360, New York (May 24, 2016, 11:49 AM ET) --

Sean Doherty

Over the last six years, there has been a growing chorus from security professionals highlighting the need for law firms to implement better cybersecurity and to take a more serious approach in safeguarding client and firm information from the growing risk of cyberbreaches. After all, in a transforming landscape where proprietary corporate information and sensitive customer data is quickly becoming the new currency, determined cybercriminals are correctly looking at targets such as law firms in the same manner as robbers go after banks. As the adage goes, the bad guys only go to where the "money" is — and for the enterprising cybercriminal, there might not be a more attractive target than the legal services industry.

Not only do these organizations represent a treasure trove of information, but historically they have been synonymous with dreadful cybersecurity practices that imperil sensitive data such as litigation strategies, attorney-client privileged communications, client intellectual property, and privacy data of employees, clients and third parties alike. Recently, the New York Times Dealbook reaffirmed digital security at law firms to be "below the standards of other industries" as well as representing a relatively higher target for cyberintrusions, citing a report from a Citigroup cyberintelligence center report.

Nowhere is the attractiveness of law firms as targets more evident than the April 2016 Mossack Fonseca hack, believed to be the most significant data theft event in history. Over 2.6 terabytes of sensitive information were exfiltrated, 1,500 times the amount of data released by the WikiLeaks scandal. Observers are expecting the total amount of information to be released will include over 11.5 million proprietary documents, approximately 5 million emails, 3 million database records, and over 2 million PDF files, mostly pertaining to the sophisticated ways in which over 215,000 companies and over 14,000 individual clients had been discreetly obfuscating wealth through front companies and intricate tax shelters.

Mossack Fonseca said its preliminary investigation determined that the attack was not the result of the actions of a trusted insider, but the fact that one of its email servers had been hacked last year. However, victimhood to a remote access attack by a determined adversary should not absolve Mossack Fonseca if it is discovered the firm neglected basic information security practices or failed to incorporate minimum safeguards necessary to protect its trove of sensitive client information. After all, in this digital age, a law firm's ethical and legal obligations to client confidentiality is now inexorably tied to the effectiveness of its IT security and information assurance programs — which must be predicated on an anticipatory approach to security threats with a focus on prevention and detection.

But what is the current state of cybersecurity in the legal industry? To calibrate, consider the findings from a 2012 study by the International Legal Technology Association.

Some key findings were:

- 78 percent of law firms did not encrypt removable media such as flash drives;
- 86 percent of law firms did not implement two-factor authentication;
- 76 percent of law firms did not encrypt email;
- 58 percent of law firms did not encrypt laptops;
- 87 percent of law firms did not implement mobile device security such as laptop-tracking technology;
- 61 percent of law firms did not deploy intrusion detection; and
- 64 percent of law firms did not deploy intrusion prevention.

A 2015 version of the same survey revealed progress on several issues, including preventative activities such as encryption, security awareness training and risk assessments.

Of note, the following stood out:

- Use of mobile device management (MDM) solutions to help organizations better secure emails, documents, and segregate data demonstrated a significant gain from the preceding year, with 52 percent of respondents indicating their firms use MDM;

- Significant improvement in deployment of encryption software covering email, laptop hard drives, and removable media;

- Security awareness training programs gained momentum with 49 percent of law firms now having them in place, including 86 percent of law firms with more than 350 attorneys.

While no doubt good news and hopefully a foreshadowing of things to come, absent regulation, firms can also commit to better defending their information by taking a simple, three-step approach.

Critical Asset Inventory

To know what to protect, you need to know what you have that is most important. To do this, you must develop an understanding of what assets malicious adversaries might want to target, as these are the most important things to defend. This basic yet important step can be accomplished through the simple act of defining and categorizing cyber assets based on their degree of sensitivity, their association to other critical assets, and understanding the value their loss could have on current and future earnings, your firm's brand reputation, and the risk to your clients' respective bottom lines and legal liabilities.

According to the 2005 revision of ISO/IEC 27001, an asset is defined as "anything that has value to the organization." Examples of assets can include intangible assets such as information routinely used and accessed by law firms, like privileged communications and client intellectual property such as patents, as well as tangible assets such as IT hardware and software. Important to note, this should also include an understanding of those systems and assets utilized by critical suppliers and other external

dependencies, but particularly shared service centers and document production services, both of which represent unique risk exposure to the legal industry.

Cybersecurity Risk Assessment

Once you have an idea of what critical assets exist, an objective and holistic cybersecurity risk assessment should be performed in order to create the necessary blueprint from which a successful risk management plan can be created. Such an assessment can identify trends, patterns, and areas of elevated risk to those assets across your holistic enterprise. A thorough assessment should include:

- A review of insider threat, mobility and travel security, and supply chain risk, which can provide valuable insight into strengths and weaknesses of the controls currently deployed to protect these areas.

- Scores to benchmark and seek maturity improvements of all the security functions performed across the firm. This includes not just an evaluation of traditional technical controls such as hardware and software, but also overarching governance and continuous cybersecurity training. As we continue to see, firms who provision their risk management resources proactively towards prevention and continuous risk assessments ultimately fare better than those who view security through the compliance audit or remediation prism.

- An analysis of how work processes and people move documents around. The content of those documents is absolutely essential and could be devastating if lost. Nevertheless, law firm employees commonly move documents from secure central repositories onto local hard drives, mail them to themselves in order to work at home, or collaborate via unsecure email. An analysis of this workflow will inform a dual focus on maintaining needed access while protecting security through common controls such as vulnerability scans, regular patching, encryption of laptops, use of a virtual private network, and two-factor authentication to protect against disclosure of assets or credentials

Development of Risk Management Plan

After a holistic cybersecurity risk assessment has been performed, the foundation of a proactive and preventative approach to security can begin to take hold.

- To start, prioritize the top vulnerabilities identified and create targeted security initiatives to mitigate them. Ensure the proper investment in and deployment of controls that are designed to prevent, detect, correct and recover from digital threats. In this regard, key controls focusing on encryption, data classification, intrusion detection and prevention, and employee education are paramount. Furthermore, accommodation for risks such as internal data theft, data leakage, data misuse, as well as social engineering must be addressed.

- Understand that a sustained commitment to security and effective risk management will be predicated on security culture, which requires not just executive-level buy-in, but support from the greater organization so that policies and procedures are not just created but also enforced, and thereby matured.

- Consider creating a security governance group which involves representatives from multiple departments such as IT, HR, finance and others. This way, policies and processes can be developed, enacted, communicated and measured as an organizational approach to security rather than one driven by the IT department. For example, HR may lead the development of training and awareness efforts and programs to mitigate employee dissatisfaction to reduce the likelihood of insider threat. Finance may draft policies requiring the authentication of requests for wire transfers, or Legal may develop standard cybersecurity language for all contracts signed with external service providers.

- Plan for the worst by developing a crisis management plan to quickly respond to a cyberattack. Multiple studies have shown that financial losses from a single cyberattack can exceed $50,000 for small businesses, and well over $1 million for large organizations. Having a quickly executable plan that includes clear responsibilities and lines of communication will help minimize the damage.

Like with all other organizations in all other industries, the threat posed from malicious adversaries in cyberspace is indeed formidable and one that requires legal firms to implement a tailored security strategy that aims to deter potential adversaries away and onto less-defended targets. For law firms, this means the adoption of a proactive and preventative footing that is centered on the idea that cybersecurity is not just an IT problem, but a greater business challenge that is required to ensure client confidentiality.

—By Sean Doherty, Secure Halo

Sean Doherty is the president and founder of Secure Halo, a Silver Spring, Maryland-based enterprise threat consultancy supporting Fortune 500 companies and the public sector. He previously served in various positions within the U.S. government and military, specializing in highly sensitive national security interests and cybersecurity-related issues.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.