Published on *The National Law Review* https://natlawreview.com

Law Firm Data Breaches: Big Law, Big Data, Big Problem

Article By:

Kathryn T. Allen

The Year of the Breach

2016 was the year that law firm data breaches landed and stayed squarely in both the national and international headlines. There have been numerous law firm data breaches involving incidents ranging from lost or stolen laptops and other portable media to deep intrusions exposing everything in the law firm's network. In March, the FBI issued a warning that a cybercrime insider-trading scheme was targeting international law firms to gain non-public information to be used for financial gain. In April, perhaps the largest volume data breach of all time involved law firm Mossack Fonesca in Panama. Millions of documents and terabytes of leaked data aired the (dirty) laundry of dozens of companies, celebrities and global leaders. Finally, Chicago law firm, Johnson & Bell Ltd., was in the news in December when a proposed class action accusing them of failing to protect client data was unsealed.

A Duty to Safeguard

Law firms are warehouses of client information and how that information is protected is being increasingly regulated and scrutinized. The legal ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to client. (ABA Model Rules 1.1, 1.6 and Comments). Attorneys also have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information, financial and health, for example.

American Bar Association's 2016 TechReport

Annually, the ABA conducts a Legal Technology Survey (Survey) to gauge the state of our industry vis-à-vis technology and data security. The Survey revealed that the largest firms (500 or more attorneys) reported experiencing the most security breaches, with 26% of respondents admitting they had experienced some type of breach. This is a generally upward trend from past years and analysts expect this number only to rise. This is likely because larger firms have more people, more technology and more data so there is a greater exposure surface and many more risk touch-points.

Consequences of Breach

The most serious consequence of a law firm security breach is loss or unauthorized access to

sensitive client data. However, the Survey shows there was a low incidence of this, only about 2% of breaches overall resulted in loss of client data. Other concerning consequences of the breaches are significant though. 37% reported business downtime/loss of billable hours, 28% reported hefty fees for correction including consulting fees, 22% reported costs associated with having to replace hardware/software, and 14% reported loss of important files and information.

Employing & Increasing Safeguards Commonly Used in other Industries

The 2016 Survey shows that while many law firms are employing some safeguards and generally increasing and diversifying their use of those safeguards, our industry may not be using common security measures that other industries employ.

1. Programs and Policies. The first step of any organization in protecting its data is establishing a comprehensive data security program. Security programs should include measures to prevent breaches (like policies that regulate the use of technology) and measures to identify, protect, detect, respond to and recover from data breaches and security incidents. Any program should designate an individual, like a full-time privacy officer or information security director, who is responsible for coordinating security. However, the numbers show that the legal industry may not be up to speed on this basic need. Survey respondents reported their firms had the following documented policies:

- Document or records management and retention policy: 56%
- Email use policy: 49%
- Internet use/computer use policy: 41%
- Social media use: 34%

2. Assessments. Using security assessments conducted by independent third parties has been a growing security practice for other industries; however, law firms have been slow to adopt this security tool, with only 18% of law firms overall reporting that they had a full assessment.

3. Standards/Frameworks. Other industries use security standards and frameworks, like those published by the International Organization for Standardization (ISO) to provide approaches to information security programs or to seek formal security certification from one of these bodies. Overall, only 5% of law firms reported that they have received such a certification.

4. Encryption. Security professionals view encryption as a basic safeguard that should be widely deployed and it is increasingly being required by law for any personal information; however only 38% of overall respondents reported use of file encryption and only 15% use drive encryption. Email encryption has become inexpensive for businesses and easier to use with commercial email services yet overall only 26% of respondents reported using email encryption with confidential/privileged communications or documents sent to clients.

5. Cybersecurity Insurance. Many general liability and malpractice polices do not cover security incidents or data breaches, thus there is an increasing need for business to supplement their coverage with cybersecurity insurance. Unfortunately, only 17% of attorneys reported that they have cyber coverage.

Conclusion

It is important to note that the figures revealed by the 2016 Survey, while dismaying, may also be extremely conservative as law firms have a vested interest in keeping a breach of their client's data as quiet as possible. There is also the very real possibility that many firms don't yet know that they have been breached. The 2016 Survey demonstrates that there is still a lot of room for improvement in the privacy and data security space for law firms. As law firms continue to make the news for these types of incidents it is likely that improvement will come sooner rather than later.

National Law Review, Volumess VII, Number 11