The Role of Encryption in Law Firm Data Security

Whether, when and how to encrypt requires a careful look at what data the firm keeps, and how much protection it needs.

David Greetham and David Levine, Ricoh USA, Cybersecurity Law & Strategy, None

August 14, 2017

This article appeared in Cybersecurity Law & Strategy, an ALM publication for privacy and security professionals, Chief Information Security Officers, Chief Information Officers, Chief Technology Officers, Corporate Counsel, Internet and Tech Practitioners, In-House Counsel. Visit the website to learn more.

Incidents over the last few years leave little doubt that hackers are increasingly targeting law firms. The data breach of law firm Mossack Fonesca, known as the Panama Papers, last April was the largest known and highest profile. The thieves took 2.6 terabytes of data, including 2.2 million PDFs, 3 million database files and 4.8 million emails.

Yet, many law firms don't use even basic encryption. In the ABA's 2016 Legal Technology Survey, only 38% of respondents reported using file encryption, only 26% use email encryption for confidential or privileged communications and documents sent to their clients, and only 15% use drive encryption.

Encryption can play a vital role in securing data, but it needs to be considered within the context of a firm's overall IT security strategy. In the Panama Papers breach, for example, the law firm's lack of the use of encryption was only one of many other security flaws, including failure to keep software patched and log-in credentials up to date. Whether, when and how to encrypt requires a careful look at what data the firm keeps, and how much protection it needs. This article explains how encryption can be used to guard against the reputational, financial and legal damage a breach of sensitive data can cause to law firms.

Examine Your Data

Legal ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to their clients. Attorneys also have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information.

To do this, firms must first understand what information they have. From that evaluation, a firm can identify an appropriate solution with acceptable risk as it applies to particular sets of data. In an ideal world, all information — including emails — would always be encrypted, whether in transit or at rest, and regardless of where it was stored. But in the real world, that's not practical because it can add cost, frustrate users, and impede productivity.

The use of encryption boils down to a discussion of acceptable risk. The appropriate level of encryption depends upon specific use cases and is a balance among many factors, including the sensitivity of the data, the need for usability and convenience in accessing and using the data, and the impact if the data were to be breached. For example, basic data that is public information, such as corporate addresses, probably doesn't need to be encrypted. Conversely, details of an upcoming transaction held in the files of a firm specializing in mergers and acquisitions needs strong protection.

Law firms must evaluate not only their own security, but also that of their vendors and third-party service providers, as well as cloud service providers. Remember that the fault that led to the 2013 Target breach, in which hackers obtained tens of millions of customer names and credit card numbers, was a third-party HVAC vendor's lack of security. Nevertheless, it was Target and its customers that suffered the damage.

At Ricoh, we ask the following questions in evaluating the data that we hold, and that third parties hold, to decide whether encryption should be used and to what extent. It's part of our overall program of best practices to ensure the security of not only our data, but most importantly, the data of our clients.

Types of Data

What kind of information do you store or transmit? Is it confidential financial information, such as IRS records, bank statements or credit card data? Do you hold any healthcare data? Do any of the laws about protection and privacy — such as Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS) — apply?

Do you or your clients need to meet the requirements of specific security certifications? If you're dealing with the federal government and store information in

the cloud, for example, you're probably required to meet the requirements of the Federal Risk Authorization Management Program (FedRAMP).

Value of the Data

How valuable might the information be to hackers? Even after the high-profile breaches of the last few years, some law firms still don't think they are attractive targets for hackers. But the ABA results belie that belief. In the survey, 14 % of respondents overall (and one in four respondents from firms with 10-49 attorneys and 500-plus attorneys) reported that their firm had experienced a data breach at some time.

The common — and faulty — assumption law firms sometimes make is that hackers only go where the money is, meaning banks or retailers. What law firms often fail to recognize, however, is that they are holding client data that could be very valuable to hackers. Just as hackers targeted an HVAC company to get at Target's data, hackers are targeting law firms to get at client data. Firms that are involved in M&A have information on upcoming transactions that is extremely valuable in the stock market.

In early 2016, for example, 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 December 2016, the FBI and the U.S. attorney for the Southern District of New York indicted three Chinese traders, alleging that they hacked into several U.S. law firms, stole millions of documents from the servers at two firms, and made more than $4 million in illegal profits from trading on the ill-gotten information.

On the other hand, it's important to balance the level of encryption against the need for ease of use and accessibility. Some types of encryption can be so cumbersome that they interfere with the operation of the firm. Use of an email encryption service, for example, can require users to log in to the service for every single email sent and received. Such hurdles sometimes prompt users to look for ways around them just so they can maintain productivity.

Location of the Data

Where is the data housed and how does it get there? Is it transmitted via a private, secure network or over the public Internet? If the latter is used for sensitive data, make sure to use encryption in transit. Is sensitive data being referenced in e-mails or in e-mail attachments? If so, they may need to be encrypted.

In some cases, the data may be physically transported, for example stored on hard disk drives and shipped. If so, are the hard drives encrypted? Are they physically

secured? There have been many instances of data breaches that had nothing to do with hacking into networks; thieves simply stole hard disk drives from the back of a truck.

Even more common are thefts or simple loss of laptops, tablets and smartphones. Are attorneys storing sensitive data on their devices? If so, they should be required to encrypt their data. Whole-disk and file-level encryption are two common ways to secure the data.

Security Practices of Vendors

Have you evaluated the security practices of your vendors, including cloud service providers? Where do your providers store your data? Is it encrypted at rest and encrypted in transit between applications (intra-application encryption)? What certifications do they meet? Some common ones are the ISO/IEC 27000 Series, the cybersecurity framework of the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA) Cloud Controls Matrix.

Is data backed up and if so where is that backup kept? How does the data get there? Is data encrypted in transit? Are backups encrypted? What type of encryption does the provider use? Who has access to the encryption keys?

Look beyond certification of the vendor's infrastructure and into its applications as well. Does the cloud service provider use third-party applications? If so, do the applications encrypt data?

Encryption is a vital part of a solid IT security program, and one that all law firms need to consider. It is the law firm's responsibility to evaluate the data and understand how to apply the appropriate level of encryption and to ensure that the data remains encrypted when appropriate at its third-party suppliers. Their business, and their clients business, may depend on it.

David A. Greetham is vice president, e-discovery sales and operations, at Ricoh USA, Inc. David Levine is vice president of information security and chief information security officer at Ricoh USA, Inc.
