NEW TECH FOR THE NEW YEAR

By Rebecca Sattin

2016 has been a tumultuous year. Woven into the headlines, however, has been a subtext regarding cybersecurity. Our presidential election has brought us discussions about email security and privacy along with concerns about the next administration's policies on encryption and surveillance. Simultaneously, concerns with security and information governance have only been growing in all industries including legal. Security experts have likened the current era in cybersecurity to the early days of flight. It began with the question "can it be done" before anyone had any idea of the myriad uses – both good and bad – for which it would eventually be used.

Comments were added to the ABA Model Rules regarding an attorney's ethical responsibility to understand technology relevant to his practice and to take reasonable means of protecting client data. Additionally, any law firm with health care or financial services clients may also be subject to regulatory requirements such as those dictated by HIPAA (Health Insurance Portability and Accountability Act) or FINRA (Financial Industry Regulatory Authority). Although not every firm has to comply with these regulatory requirements, they still may face demands from their clients. The second annual ALM Intelligence Law Firm Cybersecurity Survey indicated that "more than 70% of firms report that their clients have exerted pressure on them to increase internal security."

As a result, one topic brought to the forefront is encryption. Put simply, encryption means encoding information in such a way that only those authorized can decode it. There are a number of ways encryption technology can be implemented, many of which are quite complex. The challenge facing law firms is to find a technology that can ensure the security of client information without being so complicated that it is difficult to implement or use. Firms may be required to encrypt data both when it is being transmitted and when it is at rest.

Another topic that has been a focus for several years is collaboration and sharing. Email has become the most common method of communication, but it is not a secure way to transmit sensitive or confidential information. There are many ways that data can be encrypted in transit but the simplest products to implement

Rebecca is CIO of World Software Corporation. She was formerly at Mitchell Silberberg & Knupp LLP for 18 years, where she was Director of Information Technology. She has more than 20 years of experience in the area of law firm technology. She spoke on "Talking Technology to Lawyers" at Legal Tech Los Angeles 2012 and has spoken on various topics at many of the last several International Legal Technology Association (ILTA) conferences. She spoke at the Good Exchange conference in New York in 2014 on mobile device management. She has also served on the advisory board for LA City College's Computer Technology department. Rebecca is a graduate of Washington University in St. Louis.

secure

WORLDOX ENCRYPTION AT REST

Protect your valuable data.

AES-2048 ENCRYPTION

FOR ON-PREMISES WORLDOX INSTALLATIONS...

With encryption now a necessity due to the influx of cybersecurity risks that increase daily, this technology must be made affordable to firms of all sizes. Worldox Encryption At Rest (WEAR) works with your Worldox system of data classification and your retention policies to secure all of your data or just the data deemed to be most at risk. No costly additional hardware is required for implementation, making compliance with client or regulatory requirements attainable to all.

- Background encryption on the fly, transparent to users
- File level encryption using the AES-2048 standard
- Firm controlled encryption keys
- Secondary encryption key for super sensitive files

worldox.com
800.962.6360 | sales@worldox.com

Worldox® Encryption at Rest

and use are those that integrate directly with Outlook, making it easy to encrypt attachments on the fly prior to sending messages. Some products on the market may also include the ability to clean metadata as well as some digital rights management features that remove the ability to print or modify attachments on the fly during the send process.

There are other products whose focus is on the sharing of information that may or may not also be used for collaboration. Many of these products offer a Cloud-based repository for both the sharing and collaborative components. When evaluating such products, ensure that data is encrypted as it is transmitted to the hosted repository. Look for providers that allow the ability for the data center to reside in the country.

In some instances, it is necessary merely to provide someone outside a firm with documents in a secure manner. With the current focus on information governance, when a collaboration is occurring it is also important to ensure that there is some way to track the story of that collaborative effort. Look for products that integrate with the document management so that the entire story of a document can be found in one place.

Encrypting data at rest is another story. NIST (the National Institute of Standards and Technology) is not very specific in its definition of data at rest but they do outline four types. Their standard is written broadly and addresses many types of encryption at rest, leaving a wide range of ways in which this standard can be implemented. The four types are: full disk level, file level, database level and application level.

There are both hardware and software solutions that provide full disk encryption, but these primarily protect against loss or theft of hardware. Storage products that use hardware based encryption can also be prohibitively expensive for smaller firms. The most common threat to data comes from malware that can come through phishing attempts or one false click on a search result in a browser and full disk encryption does nothing to remediate this risk.

File level encryption implemented through an application provides a higher level of security and may alleviate some of the threats that come from malware. When implemented with a least privilege strategy for the most sensitive types of data, these types of encryption provide added layers of security.

The best way to implement encryption at rest is such that it secures data without any added overhead or complicated processes. Full disk encryption satisfies this requirement, but the aforementioned issues do not provide much more than the ability to check a box on an RFP or other client inquiries. In order to provide more robust protection, an encryption solution should allow easy access to data while access is required, returning the data to its encrypted state once files are closed.

Whether we compare the current climate to the wild west or the early days of flight, we live in a new world where we are only just beginning to recognize the technological and legislative challenges associated with protecting our data and our privacy. When implementing new technology, the end result should be first and foremost that client data is protected.