Could Data Encryption Be Your Last Line of Defense Against Hackers?

Some firms are using the technology to protect electronic communications and other files. Find out what it entails.

ERIN BRERETON
Owner, Chicago Journalist Media

With pending financial transactions, Social Security numbers and other potentially lucrative pieces of information whirring back and forth in attorney and client emails and residing in documents on servers, law firms can be particularly tempting targets for cybercriminals.

Recent research indicates they're pursuing law firms' data more aggressively. The amount of firms that have experienced a data breach rose from 14 to 22 percent between 2016 and 2017, according to the most recent American Bar Association Legal Technology survey.

Firms with 10-99 attorneys were particularly plagued with breach issues; firms with 10-49 attorneys reported the most incidents, followed by firms that employ 50-99 lawyers.

Still, acceptance of encryption has grown at a slow pace in the industry. From 2011 to 2017, email encryption use grew just 13 percent — and in 2016, it actually declined.

WHAT ENCRYPTION INVOLVES

Concerns about keeping Klein Law Group's financial and other information secure prompted

"It's not very difficult for somebody to grab an email off the internet, change an account number and send that email back on its way. The next thing you know, we're wiring money to Nigeria."

the Founder of the 10-employee Boca Raton, Florida, firm, Eric Klein, to start using encryption software several years ago.

"We do real estate closings and also have a title agency as part of our practice; hackers know lot of money is involved with real estate transactions," Klein says. "It's not very difficult for somebody to grab an email off the internet, change an account number and send that email back on its way. The next thing you know, we're wiring money to Nigeria."

When used in tandem with firewalls and other protective measures, encryption can offer firms an additional layer of protection. Essentially, the technology scrambles the content of an email or document before it's sent or stored so the text is unreadable if intercepted.

Items can later be unencrypted using two numeric keys — series of numbers that verify someone is authorized to send, save or access an item.

An attorney, for example, could send a message with software that encrypts it using a key that's linked to the attorney's identity, identifying she's the one who sent the message. When the attorney's client receives the email, he'd need to provide a separate key that the attorney had previously given him to be able to access the text.

If a hacker were to intercept that encrypted email in transit, without knowing what key to enter, its content would look nonsensical — preventing the hacker from obtaining any sensitive information it contained.

WHY SOME FIRMS CHOOSE ENCRYPTION

The American Bar Association issued new guidance last year addressing the role encryption can play in firms' ethical obligation to protect electronically stored information.

The association noted that while email messages provide a reasonable expectation of privacy in routine communication with clients, newer communication methods, such as texting, may not — making it "not always reasonable to rely on the use of unencrypted email."

Some state bars have also introduced breach-related direction. For example, Klein says that if he were hacked, he'd have to explain to the Florida Bar what his firm did to try to prevent it.

Even if attorneys don't lose their license over breach issues, the bar can, he says, potentially still reprimand them, making encryption and other security measures a worthwhile investment.

"Anyone who researches you could see it and say, 'Oh, he's been reprimanded because he didn't protect clients' information; that's not the guy I want to use,'" Klein says. "It affects your reputation — and that's what lawyers trade on."

Clients may also be a motivating factor for using encryption. Because they can face financial and other risks if information relating to their business is stolen, some are urging firms to use the technology.

Even if attorneys don't lose their license over breach issues, the bar can potentially still reprimand them, making encryption and other security measures a worthwhile investment.

When insurance, investment and talent management services firm Marsh & McLennan decided to reach out to law firms it worked with in 2012 and ask them to start encrypting email communication, a few already had encryption systems in place, according to Senior Assistant General Counsel Ronnie Brandes.

Others, she says, were happy to add the functionality.

"We work with personally identifiable and health information protected under HIPAA, so encryption and making sure data is transmitted securely is always at the forefront of the company's mind," Brandes says. "We started having these conversations with the firms we have the longest relationship with, and none of them really put up a fuss. They also saw it as a way to practice good cyber hygiene."

Heather Clauson Haughian ... says she's seen more clients request clarification about the firm's encryption and other security practices — in some instances as early as when the engagement letter is presented.

Heather Clauson Haughian, Cofounder and Chief Technology Officer of business law firm Culhane Meadows, which has offices in seven U.S. cities, says she's seen more clients request clarification about the firm's encryption and other security practices — in some instances as early as when the engagement letter is presented.

"As the legal industry is getting more educated [about encryption], so are our clients," Haughian says. "We've got [clients in] highly regulated industries that actually provide us with audit questionnaires that say: Are you doing these things? What protections do you have in place?"

WHAT TO ENCRYPT

Firms may opt to encrypt some items they feel contain particularly sensitive information and not others — all email exchanges, for instance, or possibly individual files in various locations, documents stored on servers or entire laptop operating systems.

Randolph Kahn, Founder of information consultancy Kahn Consulting, teaches a course on electronic information law and policy at the Washington University School of Law in St. Louis, Missouri. He suggests discussing what information should be encrypted as early in the relationship as possible to gauge clients' feelings.

"Have those conversations upfront so the ground rules are properly established — there's an understanding that we're going to encrypt certain kinds of conversations going forward," Kahn says.

Once the firm decides which items will be encrypted, he suggests creating a formal policy that indicates the specific ways and instances when data should be encrypted.

"Law firms shouldn't leave to chance how their lawyers evaluate and conclude when to use or not use encryption technology," says Kahn. "Mistakes happen. A policy increases the likelihood employees will get it right."

WAYS FIRMS CAN ENCRYPT FILES

Although some encryption options may require clients to log into the encryption system before they can view an email or document, some will automate the verification process if both parties have previously authenticated each other's identity.

Klein Law Group's software will send an email containing the firm's name and logo with a link leading to an online portal where a recipient can securely access a message, or it can deliver encrypted messages to known recipients with the key information to confirm Klein sent it and decrypt the message.

When the message arrives in the recipient's inbox, it looks like any other email except for a footer that lets the recipient know it's been encrypted. While that type of system may require some setup, it can be beneficial for clients who feel repeatedly keying in a password will be a hassle.

"One of the realities of encryption is it usually adds steps to the process, which for some clients is not preferred," Kahn says. "[However], encryption tools come in all varieties, colors, flavors and sizes, some of which are really intuitive and simple, and others that are not so simple."

Firms can also choose solutions that scan and encrypt content they perceive is a risk, according to Kahn, such as a birthdate. Other systems will automatically encrypt all documents and outgoing messages, lessening user responsibility to identify sensitive information.

The software Culhane Meadows chose, for instance, doesn't require firm members to indicate which individual items should be encrypted.

The fact that the encryption software would be running in the background, providing constant security support, was a major selling point for the firm, according to Haughian.

"The platform takes it off our plate so it's something we don't have to worry about," she says. "If I know I'm going to upload a document to the system in the cloud, during the transmission process, it will be encrypted in transit. I know when it's sitting in a data center, it's encrypted — there's nothing I have to do to activate that." ■

ABOUT THE AUTHOR

Erin Brereton is a freelance writer, editor and content strategist who has written about the legal industry, business, technology and other topics for 20 years.

breretonerin@gmail.com
twitter.com/erbrer09
www.chicagojournalist.com