LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

OM Feature

OPERATIONS MANAGEMENT

Removing Cyberbreach Risks

Six issues that can position your firm for a major information meltdown

Reports earlier this year that a hacker had accessed more than 50 law firms' networks may have initially seemed shocking, but it was hardly the first security snag the legal industry has experienced.

ERIN BRERETON
Owner, Chicago Journalist Media

In reality, as of 2015, roughly one in four firms with 100 or more attorneys had been the victim of a data breach, according to an American Bar Association ***survey***. Fifteen percent of all firms, regardless of size, reported a breach incident had occurred — compared to 10 percent three years before.

Yet many law firms — particularly smaller ones — often don't feel they need to worry, according to Neill Feather, President of website security solution provider SiteLock and an Online Trust Alliance advocacy group board member.

"High profile attacks can give smaller organizations a false sense of security — that they're not big enough to ward that happening to them," Feather says. "The reality is, the vast majority of attacks happen to companies with less than 100 employees, and most law firms fall into that group."

"Twenty years ago, everybody would use a desktop computer at work; now you've got multiple laptops, working from hotels, working from home, from coffee shops. There are just a lot more vulnerabilities in the system."

JACOB OLCOTT
Vice President of Development, BitSight

The ABA Commission on Ethics 20/20's 2012 comments on technology — that attorneys need to take reasonable steps to protect confidential information that's shared electronically — was a bellwether change for the industry, according to Shari Claire Lewis, a Partner at New York regional law firm Rivkin Radler LLP.

However, Lewis, who has given presentations about law firm cybersecurity risks at legal conferences and other events, notes there's still room for improvement.

"Frankly, many lawyers don't understand or underappreciate the risk of improper redaction, transmission or interference," she says. "Or they're not as familiar as they could be with the technology that protects data when it's sent back and forth, as is required in communication with each other, clients and the court."

AN AMPLIFIED FOCUS ON FIRMS

In the past five years, attackers have increasingly targeted organizations — like law firms — that are part of large companies' supply chains, according to Jacob Olcott, former Legal Adviser to the Senate Commerce Committee and current Vice President of Development at BitSight, a company that rates organizations' cybersecurity effectiveness.

The data law firms acquire during deals can, in particular, seem valuable to outside parties.

"When someone is interested in understanding the results of a [fiscal] quarter that are about to be announced, or who is filing for patents or trademarks, firms' business information makes them a hot target," Olcott says.

If employees can also access and share the information, firms' potential internal security issues, coupled with the possibility of outside attacks, make it virtually impossible to completely safeguard against all cyberrisk. But that doesn't mean they shouldn't try to.

"Nothing is 100 percent," Feather says. "Just like any other kind of risk management, you need to put steps in place to reduce the amount of risk — and make sure you're doing everything you can to protect yourself."

Proactively addressing six of the most common cyberthreats law firms face can be a good place to start.

"Nothing is 100 percent. Just like any other kind of risk management, you need to put steps in place to reduce the amount of risk — and make sure you're doing everything you can to protect yourself."

NEILL FEATHER
President, SiteLock

RISK #1: HACKERS HIT YOU WITH MALWARE

If hackers succeed in getting a firm member to download malicious software — also known as malware — and if it infects existing files and spreads a virus, then the result can range from spam being sent out from the firm, or passwords and other sensitive information being stolen.

Some industry members say ransomware, often sent as an email attachment, seemingly from a partner or client, appears to be on the rise. If opened, the ransomware can attach itself to the place all files are stored in the system and encrypt them, according to Patrick Wiley, Chief Executive Officer (CEO) of technology management, consulting and outsourcing company Aldrige.

"To get them unencrypted, you have to pay, generally in bitcoins," Wiley says. "Very recently, a potential client had to pay more than $7,000 to unencrypt its files."

Most times, the hackers will follow through and unencrypt the files once paid, according to Lewis. Yet, damage may already have been done.

"Firms of all sizes are being hit with ransomware," she says. "A law firm can only imagine the professional and public relations nightmare if it has to say, 'We're locked out of our files; we don't know when due dates are.'"

To Boost Protection: Invest in security software with malware prevention capabilities.

"Working with tools like web application firewalls are very important to make sure you're blocking attacks," Feather says.

Frequently remind firm members to watch for suspicious attachments and URLs; and to avoid ransomware woes, make sure your back-up method is effective.

One of Lewis' clients was recently able to avoid paying an unencryption fee because it had been duplicating its system daily.

"You need to have foresight and the investment in a truly independently cloned system, so when they take out one, they don't take out the other," she says. "You can just say 'Never mind, we'll go with this data.'"

RISK #2: BECAUSE OF EXTERNAL SYSTEM ACCESS, DATA PROTECTION BECOMES A PROBLEM

Remote working options have become popular in recent years. In fact, in a recent Robert Half Legal ***survey***, 69 percent of U.S. and Canadian lawyers identified flex hours and telecommuting as firms' most important retention perks.

However, home computers may not be shielded against attacks, and on-the-go attorneys are likely logging on to possibly unsecured networks.

"Twenty years ago, everybody would use a desktop computer at work; now you've got multiple laptops, working from hotels, working from home, from coffee shops," Olcott says. "There are just a lot more vulnerabilities in the system."

Portable devices, ranging from smartphones to unencrypted thumb drives, can also compromise firm-related information, if lost.

To Boost Protection: Establish a policy to protect information if a portable device is stolen, left in a cab or otherwise misplaced — such as adding a program on devices that will allow you to remotely remove key information.

"One of the best practices for bring-your-own-device [arrangements] is that all devices need to be able to be wipeable when lost," Lewis says.

Preventing information from leaving the office can also help.

"A significant amount of firms simply lock it down," Wiley says. "If you're on a firm computer, and you put a thumb drive in, it doesn't even acknowledge it."

"One of the best practices for bring-your-own-device [arrangements] is that all devices need to be able to be wipeable when lost."

SHARI CLAIRE LEWIS
Partner, Rivkin Radler LLP

RISK #3: USERS CAN ACCESS MORE INFORMATION THAN THEY SHOULD

Firms often intend to limit file viewing to the attorneys involved in a matter. But additional admin and other firm members may request — and receive — access, or just find the items are available on the network.

"Unauthorized access to documents is one of the big [risks]," Wiley says. "Internal firewalls — who should see what — [aren't always] tech-driven in smaller firms."

To Boost Protection: The best way to prevent issues, according to Wiley, is to keep the IT department closely involved in any internal group changes so document security mirrors the groups' structure.

"Usually, you see a firm and IT department get of sync when they're moving so fast no formal process exists," Wiley says. "[People] just send a quick email to an IT administrator to say someone has moved from one department or practice area to another, and you add them to the new one, but don't remove them from the old one."

RISK #4: INSIDERS POSE A THREAT TO INTERNAL INFORMATION

It would be a mistake to think law firms aren't ever the target of overseas hackers.

"They are," Lewis says. "But a lot of the time, disgruntled ex-employees are the bridge to that."

A person exiting a firm could, for example, send documents to outside parties or delete a significant amount of data.

To Boost Protection: Restricting permission to ensure only the appropriate employees have access to certain documents can help reduce the chance items will be passed on.

Wiley also recommends conducting a drill to ensure your files are backed up. Document deletion will be less of a problem if you don't have to recreate them.

"No matter how great you think things are backed up, test your storage regularly," Wiley says. "Delete a series of folders and move or hide them, and have IT put them back to make sure it can."

"Unauthorized access to documents is one of the big [risks]. Internal

RISK #5: EMPLOYEE CREDENTIALS MIGHT NOT BE CONFIDENTIAL

Sixty-three percent of confirmed data breaches involved weak, default or stolen passwords, according to Verizon's 2016 data breach ***report***.

firewalls — who should see what — [aren't always] tech-driven in smaller firms."

PATRICK WILEY
CEO, Aldrige

Some leaks are accidental — the result of an associate creating a password that's extremely easy to guess, or a partner storing their password on a note under their keyboard.

In other instances, cybercriminals may contact firm members to try to obtain access.

"They'll tell a compelling story of why an email address should be changed on an account," Feather says. "Well-intentioned people could end up providing information that leads to a breach, without meaning to."

Firm members may also innocently give out personal information to individuals they know without realizing it's not a good idea.

"Sometimes it's somebody who used to work at the firm who just needed a document or two, and a friend who's a legal secretary shared her credentials," Wiley says. "[But] that's information management wouldn't want to leave the firm."

To Boost Protection: The ***U.S. Computer Emergency Readiness Team*** suggests using the first letter of each word in a sentence for a more difficult to guess password. Encouraging users to change passwords frequently can offer increased protection.

Wiley suggests conducting regular breach exercises.

"Call a random person and say, 'Hey, this is Joe from the IT department, I need your password to be able to proceed with this issue,'" he says.

Public shaming aside, employee tests can be turned into educational opportunities.

"Send an email with a [fake file named as a] known, infected virus and say, 'Would you open this attachment?'" Wiley says. "Share the story with the rest of the firm."

RISK #6: VENDORS MAY LEAVE YOU VULNERABLE TO ATTACKS

In Target's highly publicized late 2012/early 2013 breach, attackers first gained access to the retail chain's network, according to a U.S. Senate ***report***, by obtaining credentials from an HVAC and refrigeration company Target worked with, which was able to access Target's system remotely.

Law firms may confront a similar threat.

"Firms outsource a lot of their functions," Olcott says. "If a firm uses a third-party cloud service to store data, for instance, the firm would be subject to third-party cyberrisk, as well, if the service experiences an incident."

To Boost Protection: Don't just assume companies you work with are taking all the necessary precautions.

"You're ethically required to vet your vendors," Lewis says. "If I'm hiring you to host my data, how are you going to protect my information? How do you guard your servers? How do you use encryption? It's very important to look at how the vendors are helping you do it."

ABOUT THE AUTHOR

Erin Brereton is a legal industry marketing consultant who has written about the legal industry, finance, business and other topics for more than 50 legal associations, magazines, websites and other publications.

Email
Twitter
Website