Bloomberg BNA

ABA/BNA
Lawyers' Manual on Professional Conduct™

Reproduced with permission from ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, 33 Law. Man. Prof. Conduct 574, 10/4/17. Copyright © 2017 by The American Bar Association and The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Data Security

Ransomware Make You WannaCry? Protecting the Confidential Information of Your Practice and Your Clients from Cybercriminals

By Karen Stromeyer

''Ransomware can happen to you,'' was the clear message sent by a panel at the 2017 Fall Legal Malpractice & Risk Management Conference in Colorado Springs, Colorado. The panel, Doug DePeppe, Founder of eosEdge Legal, Colorado Springs; Gawain Charlton-Perrin, Director of Risk Management at Hanover Insurance Group in Chicago Illinois; Steve Smith, Special Agent at the Federal Bureau of Investigation, Colorado Springs; and mediated by Richard J.R. Raleigh, Jr., partner at Wilmer & Less, Huntsville, Alabama, discussed the increasing instances of ransomware attacks on small-to-medium law firms and businesses.

Cyberattacks targeting consumer information have been in the news lately, such as such as the massive data breaches at Equifax and Target. However, it is increasingly ransomware, such as the WannaCry worm which crippled more than 230,000 computers in 150 countries in May 2017, that is being used against small law firms to extort payments in return for unlocking files and data that has been encrypted.

Anatomy of an attack

DePeppe provided a recent example of a typical ransomware attack: two months ago he received a call from a lawyer at a small boutique firm who had a problem – all of his computer files and servers were encrypted and he could not unlock the information. An IT person was enroute, but he had not yet been contacted by the cybercriminal. All the attorney was focused on at that point was getting his files back, as he had an important brief due in 10 days.

Karen Stromeyer is a director in the San Francisco office of Murphy, Pearson, Bradley & Feeney, where she represents lawyers and other professionals in litigation and appellate matters.

After some investigation it was discovered that the vector of the attack was when one of the firm's attorneys had been traveling and logged into the airport's Wi-Fi, and logged onto the server's remote access. This had allowed the hacker to gain access and encrypt all of the firm's files. Finally, the hacker sent an email, offering to give the key to decrypt the files in exchange for bitcoins.

So, what do you do if the unthinkable happens?

Be mindful that you have private information

Often hackers will request files be sent as an offer of proof – they will decrypt the files that you send them, to prove they have the real decryption key. However, as the files are inaccessible, the victim can't tell what information he is transmitting. This could constitute a further violation of your client's privacy, attorney-client privileged or confidential information, trade secrets, or proprietary information. Unfortunately only 50 percent of negotiations with cybercriminals are successful, so careful evaluation of the bona fides of the hacker by an experienced professional can be key.

Consider a breach coach.

A breach coach is an experienced cyber law attorney who will lead the investigation and potential negotiations with the cybercriminal, while looking after the interests of the client. The importance of this step is that it will introduce the attorney-client privilege and work product protection to the investigation, so that there is a layer of protection protecting the victim from additional disclosures of client private information, and protecting the firm from disclosure of deficiencies in its data storage and security systems.

Contact the FBI

Smith estimated that the FBI receives approximately one call per week about ransomware attacks on small law firms and businesses. Remember that you are a victim, he encouraged. Most large firms will not contact law enforcement for fear of harm to their reputations if

COPYRIGHT © 2017 BY THE AMERICAN BAR ASSOCIATION AND THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 0740-4050

the information gets out. But there are various state and federal victims' rights acts that can be of assistance.

Contact your insurance carrier

While the actual ransom being extorted is usually not covered, many cyber polices will cover support, and the hiring of various professionals to help with data recovery, forensic analysis, and system evaluation, Charlton-Perrin said. Consider tendering the claim to all of your polices: Errors & Omissions, Workers Compensation, and Commercial General Liability policies may offer various coverages.

The initial investigation would likely be covered, as would breach notification letters up to a certain amount, and any damage the attack does to the client's systems. Further, specific endorsements can usually be purchased to cover additional risks, such as reputational damage. From the insurer's perspective, it would like to be informed as soon as possible, but Charlton-Perrin recommended the first call be to the bank, the second to the FBI, then the third to him.

Evaluate if you have to notify clients of the breach.

Forty-seven states have data breach statutes that describe what type of breach requires client notification, and the type of notification. Generally, if a client's personal information tied to an account notification will be required.

Prevention and Due Diligence

Thirty states have adopted ABA Model Rule 1.1, which requires attorneys when using the internet to use due care and have protections to ensure the safety of client information—ignorance is not an excuse. The good news is that attorneys don't have to become amateur IT professionals; it's okay under this rule to hire vendors or IT professionals to evaluate and safeguard your systems. So what should law firms do on their end?

Don't look like an easy mark

Attorneys who use public email domains such as Gmail and AOL are begging to be hacked, it gives the impressions that you do not have robust security measures in place. The best rule is to try to give the appearance of a full IT department behind the firm.

Educate yourself and your staff

Attend CLEs to stay abreast of the always changing nature of the risks. Staff are often the front line of attack as they receive the bulk of the communications. Train them to exercise extreme caution when clicking on links or downloading anything to prevent infection. The general rule is when in doubt, don't click.

Backup, backup, backup

It is recommend to keep backups of all electronic information in three places, one online, one offline, and one offsite. This insures against the compromise of any system.

Simply because you are a small firm does not mean that you are immune to ransomware. Do what you can to prevent such an attack, and be proactive if you are ever the unfortunate victim.

COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC.
MOPC ISSN 0740-4050