Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Rising Ransomware Threats And Their Insurance Solutions

By **Robert Chesler**

Robert Chesler

Law360, New York (July 5, 2017, 2:25 PM EDT) -- Over the past five years, companies have become conversant with a broad range of cyberthreats. Often to their dismay, companies have learned of data breach and hacking, and phishing, spear phishing, spoofing and social engineering. Ransomware, which previously had not received as much attention in the world of cyberthreats, is now in the first rank of corporate concerns. Massive attacks like Wannacry and the attack on June 27 put everyone at risk. The June 27 attack specifically targeted a law firm, DLA Piper.

What is ransomware? Ransomware is malware that installs without the user's knowledge on the user's smartphone, computer, tablet, wearable device or other internet of things ("IoT") product. It either mounts the cryptoviral extortion attack that holds the victim's data hostage, or mounts a cryptovirology leakware attack that threatens to publish the victim's data, until a ransom is paid.

The MAR Attack

The ten-lawyer firm of Moses Afonso Ryan ("MAR") in Rhode Island recently suffered a ransomware attack, and has now sued its business interruption insurance company for its loss. Moses Afonso Ryan v. Sentinel Insurance Co., No. 1:17-CV-00157-S-PAS (D.R.I. 2017). MAR's allegations in its complaint for insurance coverage demonstrate exactly what a company must train its people not to do. The complaint recites that on May 22, 2015, an attorney received an email from an unknown source that included an attachment and then clicked on the attachment. The attachment was encoded with a ransomware encrypted virus that infected and disabled MAR's computer network. The complaint recites that MAR "was locked out of its documents, lost access, lost use, the computer network lost all functionality, was taken over and rendered inoperable." The ransom amount was $25,000. It took MAR two months fully to regain control of its system. MAR's complaint claims a business interruption loss of $700,000. MAR asserts that Sentinel paid only $20,000 pursuant to its computers and media and computers fraud coverage. In its answer, Sentinel admits that it paid $20,000 pursuant to the computers and media endorsement, and that $20,000 was the limit of that coverage.

Is coverage for the ransomware attack limited to the endorsement, or does the policy cover the ransomware attack more broadly? For that matter, is Sentinel right that the endorsement provides such limited coverage? It is impossible to tell without a review of the policy, and even then policyholder and

insurance company counsel will probably still disagree. Property policies often contain explicit exclusions for computers or intangible property that could apply. Moreover, as Sentinel noted, the policy required physical damage, and an insurance company would argue that while the system was frozen, it did not incur physical damage. But see, e. g., Gregory Packaging v. Travelers Property & Casualty Co., No. 2:12-civ-04418 (WHW) (D.N.J. 2014) (incapacitation of factory by ammonia release constituted physical damage); Wakefern Food Corp. v. Liberty Mutual Fire Insurance Co., 406 N.J. Super. 524 (App. Div. 2009) (shutting down of electric grid constitutes property damage.)

The key problem for MAR may be the sublimit of $20,000. Sublimits on key coverages are an unfortunate fact of life for policyholders. A small company that pays a small premium has little bargaining power as to sublimits. It is possible that $20,000 in computer coverage by endorsement is the best that MAR's insurance broker could obtain — although it is not impossible that if MAR should lose its coverage action, it will sue its broker. As noted, infra, most ransomware attacks are brief, and a tale of woe such as MAR's, resulting in a two-month interruption, is highly unusual.

Ransomware is Rampant

The attack on MAR outlines a typical ransomware scenario, although as discussed below, ransomware is now morphing into a variety of types of attacks. The Ponemon Institute reports that the Justice Department, as of September 2016, estimated that numerous ransomware attacks occurred each day in 2016, up 300 percent from the prior year, and the average amount companies paid in ransomware attacks was $2,500. This relatively low amount is one reason why the attacks have not garnered more publicity. Also, most attacks are brief, for example, demanding payment in 48 hours. Ponemon found that most victimized companies did not report the incident to the police for fear of bad publicity.

According to the Ponemon Institute "Rise of Ransomware" study, 57 percent of respondents believed their company was too small to be a target for a ransomware attack. As demonstrated by the attack on MAR, a ten lawyer firm, this simply is not true. Small companies are less likely to have sophisticated security or computer backups compared to a fortune 500 company. Moreover, 60 percent of companies felt that third-party application vendors like Dropbox, Facebook and Twitter, put their company at higher risk for a ransomware infection. Ponemon found that the companies that did not pay a ransom usually had a complete and accurate backup.

As in MAR, employees are the weak link in allowing ransomware into a computer system. Companies should stress education, although cybercriminals are increasingly sophisticated and it is impossible to totally eliminate human error. The IoT will make it increasingly difficult for employers to train their employees on which devices are acceptable for business and which devices are for personal use only.

The IoT tremendously accelerates the threat of ransomware. A hotel in Austria had a smart key system that ran through the hotel's computer. Hackers entered the hotel's computer system and locked all of the guests out of their rooms. The hotel quickly paid a Bitcoin ransom of about $1,600. It also incurred several thousand euros to restore its system, along with the cost of upgrading its security system.

Lessons from MAR

Every company should be backing up data at an off-site location on a daily basis in order to increase its operational efficiencies in the event the company is compromised by ransomware. This may not be possible for some law firms, which should then acquire the most effective security software. However, in view of the talents of cybercriminals, no system is guaranteed to be secure, and human error is always an issue.

Insurance policies cannot stop a ransomware attack, but can ameliorate its consequences. Cyberinsurance policies, now offered by over 60 insurance companies, should be the primary policy businesses should expect to respond to data breach and other cybercrimes, including ransomware. First, many cyberpolicies specifically provide coverage for "cyber-extortion," which would include a ransomware attack. Insureds need to be very cognizant of coverage triggers and sublimits when they are evaluating one cyberpolicy to another, as this can affect coverage greatly in the event of a ransomware attack. A sophisticated broker is a necessity. Law firms must review the breadth of their professional liability policies and consider purchasing cyberinsurance.

Many such policies specifically provide coverage for "crisis management," which would include hiring a PR coach to carefully craft a message to the public about the breach the company had just incurred. This coverage also provides assistance in finding consultants, conducting a forensics investigation to determine the extent of the breach, and handling publicity issues. This has proven to be an extremely important coverage.

Both the frequency and severity of ransomware attacks have dramatically increased over the course of the past year. A cyberpolicy, tailored to the company's needs, is the most cost effective tool for addressing the financial, operational and reputational consequences of a ransomware attack.

Robert D. Chesler is a shareholder at Anderson Kill PC's office in Newark, New Jersey. He is a member of the firm's cyberinsurance recovery group.