LAW360®

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

Will Crisis Management Insurance Cover Ransomware?

By **Jeffrey Weinstein and Bruce Kaliner** (January 17, 2018, 4:44 PM EST)

Jeffrey Weinstein

"Malware" and "Ransomware" recently have entered the public lexicon and consciousness, though many people still do not understand what they are or how they differ. "Malware" is shorthand for malicious software and generally refers to any software that is designed to infect a computer with malicious intentions. Viruses, worms, adware, bots, spyware, wipers, Trojan horses, etc. are all types of malware.

Ransomware is a form of malware that is designed to encrypt computer data without the initial knowledge of the user. WannaCry, ExPetr, Samsam, CryptoLocker and Bad Rabbit are examples of ransomware attacks. After delivery, the ransomware encrypts the data or files on the infected computer or network, which essentially "locks out" the user from accessing the infected data, files or systems. The "perpetrator" of the ransomware then demands a ransom payment from the user to regain access, either by providing a program to decrypt the files of by sending a decryption key.

Bruce Kaliner

An unfortunate attribute of most ransomware is its ability upon infection to quickly spread within a company's global network. When this happens, the effect on business operations can be immediate and have a significant negative impact. Fortunately, many companies now have implemented contingency plans for ransomware attacks, but this does not thwart future attacks from being launched.

According to a May 2017 CBS News article,

> The WannaCry attack crippled computers in at least 150 countries, causing financial and economic losses that could potentially reach into the billions of dollars, making it one of the most damaging incidents involving so-called ransomware.[1]

Ransomware should not be confused with destructive malware or "wipers" that are designed to delete or overwrite computer data, such as the Killdisk, BlackEnergy and Shamoon. In June 2017, "NotPetya," masquerading as ransomware, turned out to be destructive malware, as it was designed to permanently encrypt data.[2] In other words, whereas most "ransomware" does permit the victim to recover the original data upon payment of a ransom, NotPetya purported to provide the victim with the same opportunity, though in reality the data was permanently encrypted before the victim even knew its computer was attacked.

According to the U.S. Justice Department,

> Ransomware is the fastest growing malware threat, targeting users of all types — from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. … Ransomware

> targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.[3]

Interestingly, a ransomware attack can be differentiated from cyberextortion. The Federal Bureau of Investigation, Internet Crime Complaint Center ("IC3") defines extortion as:

> … an incident when a cyber criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is often used in various schemes reported to the IC3, including Denial of Service attacks, hitman schemes, sextortion, Government impersonation schemes, loan schemes, and high-profile data breaches. Another tactic exploited in extortion schemes is the use of virtual currency as a payment mechanism. ...[4]

It has become more common for companies to seek insurance coverage for cyber incidents, and the market now offers many different products that incorporate or are focused on cyber risks; however, because of the massive financial impacts arising from the recent wave of global ransomware attacks significant claims have also been made under traditional policies, such as first-party "all-risk" property, D&O and crime. In particular, the massive financial impact from the NotPetya attack has placed a focus on "crisis management" policies for kidnap, ransom and extortion ("KRE") incidents.

Because a typical "extortion" definition in a KRE policy requires there to be a "ransom" demand and/or payment, and since NotPetya has been characterized (or perhaps mischaracterized) as a "ransomware" attack, some insureds are taking their KRE policies off the shelf to see how, if at all, these policies may respond.

Victims of NotPetya first found out they were infected when their computer screen revealed this type of message:

> Oops, your important files are encrypted.
>
> If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recovery your files without our decryption service.
>
> We guarantee that you can recover all your files safely and easily. All you need to do is submit payment and purchase the decryption key.
>
> Please follow the instructions:
>
> 1. Send $300 worth of Bitcoin to the following address: ….

Upon receiving this message, the recipient essentially had three choices: 1. Do nothing; 2. Take steps to recover the data or restore the data from backup rather than paying the ransom; or 3. Pay the ransom and hope that the perpetrator would send a "key" to unlock the data (under the assumption the malware at issue allows decryption). None of these choices was desirable. And, early investigations revealed that the ransom mechanism in the pop-up screen was not even functional, which made the NotPetya attack particularly insidious.

The "typical" or traditional KRE policy can cover a multitude of events, including kidnap, extortion, hijack, hostage crisis, assault, evacuation, etc. A typical attribute of these policies is that the insured is the intended victim of the triggering event. In the past few years, some insurers have adapted such policies to include as part of extortion coverage the unauthorized entry or introduction into an insured's computer system by software instructions that are designed to alter, damage, delete, destroy or change the insured's computer system. But, such an extortion incident still included the express requirement that a threat be communicated to the insured by person(s) who demand a ransom as a condition for not carrying out or ending the extortion incident.

A common example of a cyber extortion event would be a computer hacker who communicates a direct threat to a particular company and advises that he or she will break into the company's computer system and introduce malware that will delete all email or will steal and release proprietary / commercial information that can harm the company, unless a ransom is paid. In essence, a threat for future action against the company is being made with the condition that the ransom payment will end the cyber event (akin to a kidnap victim being released upon payment of the ransom).

With ransomware, however, the introduction of the malware to encrypt the data has already taken place before a threat is even made. And with NotPetya, the irreversible encryption to the data had already been done. The "threat" is then computer generated — the message screen with no human interaction. The ransomware infection itself is also usually happenstance to the victim, as it is not directed at one company but is designed to spread and infect, as what happened with the NotPetya ransomware. In short, a ransomware event does not fit neatly into the criteria checklist of an "extortion" under many KRE policies.

In analyzing whether a cyber ransomware incident may constitute an "extortion" under a KRE policy, the following questions may become relevant:

- Had the infection already been fully accomplished (i.e. the encryption of data) before the ransom demand was made (i.e., the computer screen message)?
- Can the continuing lockup of the data constitute the requisite future harm?
- Was the ransomware extortion message computer generated, so that the perpetrator(s) does not even know of the malware delivery and infection to a particular company?
- Was the only "contact" with the insured the computer generated ransom message? Would a computer message that is written as part of the malware code constitute a ransom demand?
- If the ransomware infects and encrypts network servers, but there is no corresponding ransom message, is this still an extortion event?
- Would the incident be an "extortion" if a ransom payment cannot actually be made because the virus is destructive malware, but the insured does not know this when reading the computer generated ransom message?
- If the insured receives the computer generated ransom message, but knows the particular variant of malware involved will never decrypt the data (the variant is destructive malware), is this still an "extortion" incident or another type of cyber extortion?
- If the insured never intends to make payment for whatever reason (i.e. has backup, refuses to be coerced, etc.), has the ransom payment requirement been met?
- If the ransomware simply encrypts the computer data, but does not delete or overwrite the data, is that considered physical damage to property?

KRE policies have been around for years and have many variations in wording and structure. They are now under increased scrutiny by insureds seeking potential coverage because of the recent spate of ransomware attacks. Moreover, because cyber-mischief-makers are becoming more inventive in the ways to wreak havoc, a fact-intensive inquiry will often be necessary to determine if the KRE policy at issue has in fact been triggered or, if it has, how far the policy would go to cover ransom-related expenses. KRE insurers are now also retaining forensic computer consultants as part of their investigation/adjustment team, in order to gain a better understanding of mechanism of the cyber attack.

Whether "ransomware" or other "malware" incidents will be considered a new form of "extortion," rather than just an unfortunately growing list of cyber crimes, will require a detailed understanding of these incidents and how KRE policies work.

Jeffrey S. Weinstein and Bruce R. Kaliner are partners at Mound Cotton Wollan & Greengrass LLP *in New York City.*

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See https://www.cbsnews.com/amp/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[2] See US-CERT Alert (TA17-181A) Petya Ransomware at https://www.us-cert.gov/ncas/alerts/TA17-181A (last updated on July 28, 2017) and NCCIC Malware Initial Findings Report — 10130295 at https://www.us-cert.gov/sites/default/files/publications/MIFR-10130295.pdf (dated June 30, 2017).

[3] See "How to Protect Your Networks from Ransomware," at https://www.justice.gov/criminal-ccips/file/872771/download at p. 2.

[4] See "2016 Internet Crime Report," at https://pdf.ic3.gov/2016_IC3Report.pdf (citations omitted) at p. 13.