CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW

NOVEMBER 2019

PREPARING FOR RANSOMWARE ATTACKS

In-house lawyers should play a leading role in helping to protect their companies from this fast-growing threat.

BY KURTIS SUHS

Ransomware is getting a lot of ink these days. And for good reason. The threat is real. According to a recent U.S. Department of Homeland Security (DHS) briefing, attacks increased by a whopping 250 percent, year over year, in 2017 and caused $5 billion in damages that year. Every 40 seconds a business is targeted, and all major operating systems have been hit. Fully 60 percent of all malware payloads contain ransomware.

Lawyers have a very important role to play in helping clients prepare for and weather attacks. But before we explain how, let's take a closer look at the different ways that ransomware can cripple companies.

More than 400 families of ransomware have been identified, but there are three main types that usually crop up.

Crypto ransomware is a class of malware that targets and infiltrates a victim's device to encrypt valuable files. Once the files are encrypted, the attacker demands that the victim pay a ransom, often within a time limit, before the records can be decrypted and recovered. Without the decryption key held by the attackers, the victim loses access to all of the encrypted files.

An example: the CryptoLocker attacks of 2013-2014. This attack used a Trojan Link that targeted computers running Microsoft Windows. The malware propagated via infected email attachments, and, when activated, it encrypted files and demanded payment in bitcoin to decrypt them.

Another variety is **wiper ransomware**. Here the attacker erases files or the hard drive of the infected computer, with no means of recovery unless a ransom is paid by the victim.

A notorious example was Petya. This malware, which appeared in 2017, would reboot a victim's computer and encrypt the hard drive's master file table, rendering the master boot record inoperable. Petya would replace an encrypted copy of the master boot record with its own malicious code, which displayed a ransom note, leaving the computer unable to boot.

Finally, there is **locker ransomware**. With this type of malware, the attacker locks out users from their systems. A message is often displayed when a user starts up a computer, stating that the user is involved in illegal activity involving pornography or software piracy, and must pay a fine to avoid legal action.

A well-known example was LockeR, a virus that, after infiltration, encrypted most stored data. Following successful encryption, LockeR placed a "How to Decrypt Files" message on the desktop, informing victims what to do next.

Cyber Special Ops, LLC

Lawyers Can Start With Clients' Insurance

Legal counsel can help their clients prepare for and defend against ransomware attacks in a variety of ways. A good place to start is with their insurance.

Attorneys should assist the company's risk managers to examine commercial property and casualty policies for potential coverage. This review should include both the cost for data restoration and the payment of the extortion demand. Today, many stand-alone cyber insurance policies will provide payment in either cash or cryptocurrency, which is often required by the hackers. Other policies that may come into play include kidnap and ransom insurance, for the payment of the extortion demand, or property insurance for the costs to restore the data.

Most stand-alone cyber insurance policies define ransomware as an attack that interrupts or threatens to interrupt the network through a malicious attack, or disseminates, divulges or encrypts data. Legal counsel should ensure that the cyber insurance policy also provides coverage for an attack against the insured's own intellectual property and trade secrets. If the policy doesn't include coverage for intellectual property and trade secrets, legal counsel should amend the policy by endorsement to carve back this coverage.

A related coverage issue is what happens if the decryption key fails to restore the data. DHS has noted that between 5 and 10 percent of companies that paid the ransom demand didn't get their data back. Is the insurer willing to modify the insurance policy so that if the company pays the ransom but doesn't recover its data, it doesn't suffer the full loss in the policy? One solution is to modify the erosion of limits to allow the insured to pay an additional premium, while the insurer recognizes a loss of no more than 50 percent of the failed ransom payment. Legal counsel should work with the company's risk management department and the insurance broker to seek clarification from their insurer for this claim scenario.

And while we're talking about risks, lawyers can help in another area. For publicly traded companies, legal counsel should carefully review in advance all press releases, financial statements and other documents filed with the SEC involving cybersecurity risks and incidents. They should do so to ensure that the company doesn't unnecessarily divulge information that makes it an inviting target for criminals. For instance, the mayor's office of a major U.S. city that was recently hit by a ransomware attack publicly stated that the city would purchase its first cyber insurance policy, with a $20 million limit and $1 million deductible. It isn't hard to imagine that this announcement was read with great interest by people who don't have the city's best interests at heart.

Review the Contracts of Service Providers

When lawyers focus on data protection, they need to think beyond the confines of their own companies. They should carefully examine contractual provisions related to the company's service providers as well. Recently, one of the most established providers of legal case management software for law firms was hit by ransomware, which resulted in a service outage.

Lawyers need to examine service provider contracts to ensure that they include strong and effective provisions on data privacy and security. These should specify that service providers maintain reasonable and compliant administrative, technical and physical safeguards to protect data.

In the event of an outage, do clients have any contractual remedies from the inability to access data? Legal counsel should require the service provider to purchase and maintain errors and omissions insurance and cyber insurance with limits enough to protect their client.

To Pay or Not to Pay?

The big question that companies need to consider is whether, in the event of a ransomware attack, they will be willing to pay.

In October 2019, the FBI's Internet Crime Complaint Center (IC3) released a public service announcement stating that broad, indiscriminate ransomware campaigns had sharply declined. However, losses from sophisticated and targeted ransomware attacks have increased significantly. According to one firm that specializes in ransomware attacks, the largest ransom that it has seen in the United States is $50 million.

The FBI doesn't advocate paying a ransom. One reason is that the agency does not favor rewarding the bad guys. Also, the FBI notes, paying doesn't guarantee that an organization will regain access to its data. In some cases, victims that paid were never provided with decryption keys. In addition, because of flaws in the encryption algorithms of certain malware variants, victims may never be able to recover some or all their data, even with a valid decryption key.

So what should a company do? Legal counsel can help the organization by working with their information security team in implementing policies and procedures to help mitigate cyber risk well ahead of an incident. This planning should include weighing the pros and cons of paying a ransom and evaluating all options to protect shareholders, employees and customers.

Ultimately, the management of each company must decide for itself. But lawyers can help them think through the issues. And if they are wise, they will do so long before the company is under the intense pressure of an actual attack.

Kurtis Suhs *is the Managing Director of Cyber Special Ops, LLC bit.ly/32uL697, a Georgia-based company that he founded to advance cybersecurity by using specialized teams and risk management techniques to prepare for and respond to a cyber event. He has over 33 years of experience in the insurance and financial services sectors, and helped launch the first cyber insurance product in 1997. Using the concierge medicine model, Cyber Special Ops provides guaranteed access to highly credentialed third-party providers for a modest annual membership fee.*