Lowenstein Sandler

Insurance Recovery

November 5, 2020

# Health Care Facilities Are Under Cyberattack; Cyber Insurance Provides a Valuable Defense

By Michael D. Lichtenstein and Lori Kahn

U.S. hospitals, already on the front lines of fighting the coronavirus pandemic, are now facing viral attacks by cybercriminals. More than 20 U.S. hospitals and health care organizations have reported their data being held hostage by ransomware, and federal agencies have warned that hundreds more U.S. health care facilities are at risk for cyberattacks. In the face of these alarming predictions, independent security experts describe the recent assault on the U.S. health care system as the most significant cybersecurity threat ever seen in the United States.

In September, over 200 U.S. facilities of a major hospital chain were crippled by a ransomware attack, creating chaotic conditions including mounting emergency room waits and failures of wireless vital-signs monitoring equipment. According to one cybersecurity firm, the Russian criminal gang responsible for the recent ransomware attacks is purposely targeting and disrupting U.S. hospitals, forcing them to divert patients to other health care providers and producing prolonged delays in critical care. The cybercriminals use ransomware to scramble data that can be unlocked only with software keys provided after the target of the cyberattack pays up.

**Ryuk on the Rise**

Cybercriminals launching attacks on health care facilities are mainly using a strain of ransomware known as Ryuk, which is seeded through Trickbot, malware that basically finds its way into a network and, once inside, plants ransomware such as Ryuk. For years, ransomware has targeted hospitals because locking up a health care organization's digital systems can threaten patient care and create maximum urgency to pay up and recover. But the current spree of infections marks an alarming shift in how aggressive financially motivated ransomware groups have become and how far they are willing to go. Private security experts say that cybercriminals are demanding ransoms in excess of $10 million per target and that criminals on the dark web are discussing plans to infect hundreds more hospitals, clinics, and other medical facilities.

Increasingly, ransomware criminals are first stealing data from targets before encrypting networks and then using the data for extortion. The criminals often sow the malware weeks before activating it, waiting until they believe the highest payments can be extracted. Thus, a major concern is that hundreds of organizations may have already been compromised by attackers, and that ransomware or the means to deploy it is lurking until hackers decide to trigger it.

**Network and Information Security Insurance Coverage (Cyber Insurance)**

There is some good news: The payment of a "ransom" may be covered by insurance. Network extortion coverage is available under insurance policies that are specially designed to address cyber risks and, sometimes, may be covered under professional liability insurance policies. Network extortion is typically defined as a credible threat by a third party, directed at the insured, demanding money or other valuable consideration in exchange for (1) returning, or refraining from disclosing, using or destroying, confidential information in the insured's care, custody or control; (2) not publicizing that the insured's network has been compromised; and (3) not impairing, altering or destroying the

insured's network (local or area-wide network operated by the insured). A network extortion expense is typically defined as any reasonable and necessary expense incurred by an insured to respond to the network extortion threat, including the payment of money. The above-discussed Ryuk attacks satisfy this definition.

Payment or reimbursement of ransoms paid are not automatically covered. First, many policies require that any payment of ransom be made along with, or at the direction of, a law enforcement agency investigating the network extortion. Thus, law enforcement involvement from the outset is critical. Second, a ransom demand is subject to strict reporting requirements. Many policies require **near immediate** (often within three days) reporting of any network extortion event. Third, all costs, including the cost of the ransom, often must be incurred within a specified period (typically six to 12 months), calculated from the date of the initial demand. Fourth, the insurer must consent, in writing, to all payments or other expenses related to the ransom demand before such expenses are incurred. Carriers also may require the insured to provide a detailed proof of loss before any reimbursement is made. Consider consulting experienced coverage counsel to guide you through the claim process.

Insurance carriers will not always agree, or be required, to advance network extortion costs and instead will reimburse these costs after they are paid. A 30- to 60-day lag time for reimbursement is common. But with true financial hardship, an advancement of certain costs may be negotiated with the carrier. Finally, insurance carriers often require that the insured not disclose the existence of extortion insurance coverage in order to reduce the likelihood that the insured will become a target specifically because it has network extortion insurance coverage.

**An Ounce of Prevention**

The best way to avoid these costs is to take basic steps to prevent becoming a victim of cyber extortion in the first place. For example, (1) protect your computer system with a firewall and antivirus/antimalware software, (2) regularly back up all data, (3) confirm that your operating system and software are patched and up to date, and (4) beware of email phishing attacks. Providing frequent reminders to your internet users about the risks of cyber extortion and phishing is also an excellent defense. The good news is that many cyber policies provide risk management services that can help guide you in this process before you become a victim. Policies may also provide coverage to upgrade your network after a ransomware attack in order to reduce the risk of a future attack. This is important because most policies will not pay repeated demands for payment made by the same extortionist or group of extortionists.

**A Word of Caution**

To avoid falling victim to an unreimbursed cyber loss, there are a few important things to know. First, payment of ransom is not a guarantee that the criminal will release your software and data unharmed. In fact, many businesses have been victims of repeat attacks. Second, you should immediately alert the FBI when you are a victim of a cybercrime. Third, premiums for network extortion coverage, and cyber insurance generally, are on the rise, so the longer you wait to purchase coverage, the more expensive that coverage is likely to be. Fourth, there are many forms of cyber insurance offered by many insurance companies, so you should work with an experienced insurance broker and coverage counsel when purchasing coverage to make sure you get the most comprehensive insurance for your risk profile. And fifth, for many U.S. businesses, it may violate U.S. law to pay money to certain international criminals. In October, the U.S. Department of the Treasury's Office of Foreign Assets Control advised that companies may violate U.S. sanctions laws if they make ransomware payments to certain cybercriminals. Be certain to consult a qualified attorney before you pay ransomware, or you may trade one problem for another.

***To see our prior alerts and other material related to the pandemic, please visit the Coronavirus/ COVID-19: Facts, Insights & Resources page of our website by clicking here.***

# Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

**MICHAEL D. LICHTENSTEIN**
Partner
**T: 973.597.2408**
mlichtenstein@lowenstein.com