KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Businesses and Their Insurers Face Threat from Ransomware, *National Underwriter*

National Underwriter recently published an article written by **Marc S. Voses and Chang Liu on the threat from ransomware to businesses and their insurers.**

Recent cyber extortion attempts use software that encrypts an organization's computer system, making them inaccessible, which causes all kinds of problems. Increasingly, companies and organizations are experiencing cyber attacks that involve extortion plots.

While insurance can mitigate this risk, the coverage available is limited. This is why frank discussions between policyholders, brokers and underwriters is key to understanding this exposure and the insurance products that are available to respond in the event of an incident involving ransomware or other extortion tools in cyber criminal's quivers.

Cyber Extortion Plots

Recent cyber extortion incidents share some common characteristics: They often use ransomware □ a type of malware that infects the victim's computer system by disguising itself as normal files or links. This malware could cause serious damage and trigger potential liability to third parties by encrypting the files on the victim's computer system, rendering them inaccessible. Oftentimes, the perpetrators are located in foreign countries that are difficult or impossible for the law enforcement to pursue.

Ransomware typically propagates as Trojan files □ malware disguised by shell software to avoid being detected by firewalls and anti-virus programs. Once the ransomware enters into the target's computer system through a click on an infected link or by downloading an infected file, the ransomware will encrypt files with a strong encryption that could be impossible to decrypt without the key. Unlike other cyber attacks, the goal of cyber extortion is not to damage the target's system or steal data, but rather extorting payment from the victim. Payment is almost always arranged in bitcoin, which is a virtually untraceable currency akin to a bearer bond.

In addition to requiring payment of money, a ransomware attack could result in liability if the computer system breach is severe and involves key operating data. For example, if a hospital lost access to its computer systems, patients' live may be at risk. In other industries, the loss of control over computer systems could mean loss of profits, property damage resulting from the inability to control manufacturing equipment, or the inability to gain access to proprietary information, including trade secrets, confidential clients' files or consumers' personal data. Of paramount concern is the potential for the loss of reputation following a ransomware attack and the possibility for copycat attacks.

Several recent cyber extortion incidents have targeted hospitals and other healthcare providers. For example, on Feb. 17th, Hollywood Presbyterian Medical Center, located in Los Angeles, paid the equivalent of $17,000 in bitcoin to hackers that infiltrated and denied access to the hospital's computer network. The malware used by the hackers locked down the hospital's computer system by encrypting its files. After paying the ransom, the hospital obtained the decryption key and regained control of the system.
Similarly, on March 28th, MedStar Health, a nonprofit healthcare organization headquartered in Maryland, was also attacked by ransomware. Although MedStar denied there was any significant impact because they quickly shut down their computer system, some employees said that the virus still disabled access to patients' records. The hackers demanded 45 bitcoins (the equivalent of about $19,000) in exchange for the decryption key. In this case, however, MedStar said that it did not pay the ransom.

This was also the case with Alvarado Hospital Medical Center in San Diego that was attacked by ransomware causing “disruptions” to the operation of the hospital on or about March 31st. The hospital said that it resolved the issue without paying the ransom.

Cyber extortion plots are not exclusive to healthcare providers, and hackers are expanding into private companies and government agencies.

In October 2015, a British telecommunications company, TalkTalk Group, sustained a significant cyber attack involving an extortion plot. Unauthorized parties gained access to personal and banking information of 156,959 customers and demanded that the company pay a ransom. Although TalkTalk did not disclose the specific amount of the ransom, news of the plot coincided with a stock price drop of 10%. Clearly, cyber extortion may cause collateral damage in addition to the ransom demanded.

On April 4th, hackers breached the computer system of the municipality of Plainfield, N.J., and demanded a bitcoin payment of about $750. The breach may have been caused by an infected hyperlink that resulted in the encryption of the files in the computer system. The city lost access to two of its computers allegedly containing over 10 years of sensitive files.

Regulators and business associations have realized the potential problem of cyber extortion. In November 2015, the Federal Financial Institutions Examination Council issued its “Statement on Cyber Attacks Involving Extortion,” which pointed out that cyber extortion could create risk of liquidity, capital, operational, compliance and reputational risks to financial institutions resulting from fraud, data loss and disruption of customer service.

Mitigating losses through ransomware coverage

Various insurance products can effectively mitigate cyber extortion losses. Some products contain extortion liability coverage, pursuant to which insurers will reimburse policyholders for losses resulting from a cyber extortion incident.

Understandably, limits are typically restricted because of the moral hazard created by providing such coverage. The concern being that fraudulent cyber extortion incidents could occur with the involvement of the insured. When coverage is available, it will frequently cover the costs of investigating and responding to the incident.
Some insurers will even offer reputation protection coverage and file recovery costs in the event the insured elects not to pay the ransom or when the decryption key is not delivered after payment of the ransom.
Work with insurers

The risk of a company, government agency or other organization falling victim to a ransomware incident is increasing because the shotgun approach taken by criminals to find victims.

While the creation and proper implementation of a ransomware plan is crucial to surviving such an incident, the majority of entities are simply unprepared for this emerging risk that is increasing in frequency at an alarming rate.
Policyholders must work together with their broker and insurers to understanding the nature of this risk and engage in meaningful discussions of how to mitigate the associated risks. Insurers have a wealth of information that can assist entities prepare for this evolving threat and are developing new products to address potential losses in the event someone in your organization clicks on a link that looks innocent enough at the time.