SOCIUS

Your money or your data!

A Discussion of Ransomware

By: Kevin Kershisnik, Laura Zaroski & Cynthia Zimmerman,
Socius Insurance Services

Your client, ABC Corp. is going about their business and then they get this message:

The above is a typical ransomware message according to a recent Symantec Security Response report. What's next? Pay the "ransom" and move on? Ransomware is a type of malware or malicious software, that is designed to block access to a computer or computer system until a sum of money is paid. After executing ransomware, cyber criminals will lock down a specific computer or an entire system and then demand a ransom to unlock the system or release the data. This type of cyber crime is becoming more and more common for 2 reasons:

1. Cyber criminals are become increasingly more organized and well-funded.
2. A novice hacker can easily purchase ransomware on the black market.

According to the FBI, this type of cyber crime is increasingly targeting companies, government agencies, as well as individuals. The most common way that criminals execute their evil mission is by sending attachments to an individual or various personnel at a company. The busy executive proceeds to open up the file, sees nothing, and continues with his work day. However, once the file has been opened, the malware has been executed and Pandora has been unleashed from the box! Now that the malware has been unleashed, a hacker can take over the company's computer system or decide to steal or lock up key information. The criminals then make a "ransom" demand on the company for a certain dollar amount. The ransom is usually requested in bitcoins, a digital currency also referred to as crypto-currency that is not backed by any bank or government but can be used on the internet to trade for goods or services worldwide. One bitcoin is worth about $298. Surprisingly, the amounts are generally not exorbitant (sometimes as nominal as $500 - $5,000 dollars). The company then has the choice to pay the sum or to hire a forensics expert to attempt to unlock their system.

The best way companies can attempt to guard against such cybercrime attacks is by educating employees on the prevalence and purpose of malware and the danger of opening suspicious attachments. Employees should be advised not to click on unfamiliar attachments and to advise IT in the event they have opened something that they suspect could have contained malware. Organizations should also consider backing up their data OFF the main network so that if critical data is held hostage they have a way to access most/part of what was kidnapped. Best practices also dictate that company systems (as well as individual personal devices) be patched and updated as soon as the upgrades are available.

Finally, in the event you are a victim of a ransom attack, you would need to evaluate whether or not that compromise of your data/system also constitutes a data breach incident. If the data hijacked is encrypted, notification is likely not necessary (as the data would be unreadable by the hacker). However, in the event the data was not encrypted, or that you cannot prove to the authorities/regulators that it was, notification to clients or individuals is likely necessary.

TAKEAWAY:

Cyber extortion is more prevalent than most people realize because such events are not generally publicly reported. In order to protect against this risk, we recommend that companies employ best practices with respect to cyber security and that they consider purchasing a well tailored cyber policy which contains cyber extortion coverage. Such coverage would provide assistance in the event a cyber extortion threat is made against the company, as well as fund the ransom amount in the event a payment is made.

Please feel free to contact your Socius producer if you would like to discuss cyber extortion coverage.