RANSOMWARE – IS YOUR FIRM VULNERABLE?

It's one of your worst nightmares: you turn on your computer, and there's a ransom note on the screen. Since your firm is working from home due to COVID-19, the attacker has used your computer to gain access to the firm's entire network resulting in a complete lockdown. Unfortunately, it appears that your computer may be the proverbial "patient zero." After you collect yourself and contact your managing partner, what should you do? Ideally, your incident response plan will guide your firm's next steps which should include immediately contacting your cyber and professional liability carriers for guidance and support.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software (malware) that attempts to extort money from victims by denying access to a computer system or files. The most prevalent form of this malware, crypto-ransomware, encrypts files that can only be decrypted with a key held by the malicious actor. Ransom payments, however, do not account for all the costs associated with a ransomware attack.

Some malware is expressly designed to harvest personal and proprietary information before dropping the ransomware. Once successful at infiltrating your system, the threat actor will collect personal data, passwords, mail files, browser data and more. This type of information can give the attacker access to important information, including personal and business bank accounts, personal or work-related email correspondence, personal and business data. Getting access to this kind of data can have severe business consequences.

Ransomware is evolving into a new type of threat where cybercriminals are not just encrypting data but are also stealing it and threatening to release it on the internet. Recently, a small firm in Texas refused to pay a ransom and had its data exposed by the cybercriminals, including fee agreements and diaries from personal injury cases. These new extortion attempts are no longer only about getting data back, but also about the risk of proprietary data being exposed or sold to other threat actors.

LAW FIRMS AND NETWORK EXTORTION

Law firms, whether large or small, are prime targets for cybercriminals, who view them as warehouses that can provide access to employee identification data, banking information, trade secrets, non-public details on client transactions and other highly sensitive information.

When a law firm is the victim of a ransomware attack, paying the ransom is not the sole consideration. Other risks include missed deadlines (including statutes of limitations), compromised client information, exposure of the firm's proprietary information and damaged reputations.

Lawyers and law firms have ethical obligations under the rules of professional conduct in their jurisdictions to competently represent their clients, to protect their clients' confidential information, and to supervise and train their staff on cybersecurity policies.

Many legal malpractice policies offer some coverage in the event of a ransomware attack. This coverage, however, can be limited and is unlikely to cover but a fraction of the costs necessary to respond to a ransomware event. Ideally, a law firm should purchase a stand-alone cyber policy which provides coverage in the event of Network Extortion. Such a cyber policy can reimburse Insureds for the expense of a ransom paid to decrypt data or to secure the return of stolen data.

If your firm is hit with ransomware:

Do:

- Consult your Incident Response Plan
- Contact your cyber and professional liability carriers
- Remove the infected system from the network
- Preserve all electronic artifacts

Don't:

- Shut down or reboot infected systems
- Communicate with the threat actor by yourself or have your local I.T. provider contact the threat actor
- Wipe out anything on your Network

AUTHOR

Brenda M. Hamilton
Senior Claims Analyst, Cyber Claims Response Team
North American Claims Group

QUESTIONS? Contact your local Allied World Underwriter. **alliedworldinsurance.com**