ERRORS & OMISSIONS
RISK MANAGEMENT ALERT

Ransomware Attacks are on the Rise; Don't Be a Victim of Cyber Extortionists

by **Thomas Casella,** JD, MBA, SCLA
Senior Risk Management Specialist
Utica National Insurance Group

Ransomware[1] attacks, also known as cyber extortion, are on the rise. As these attacks increase in frequency, ransom demands are increasing as well. More particularly, such demands are estimated to have nearly doubled in 2020 over the prior year[2]; the average ransomware demand is $233,817[3]. If your computer system is compromised by ransomware, it can cause delays in conducting your business, a loss in profits, increased expense in responding to the breach, and may impact your business's good will if personally identifiable information ("PII") is exfiltrated by the hackers.

Although ransomware attacks are increasing, there are steps you can take to protect your computer system from the attempts of hackers to encrypt, compromise and/or steal your data, as well as help you rebound quickly in the event your computer system is encrypted by hackers:

Staff education on malware and system vulnerability

- You and your staff need to be aware of what files and links you are accessing on your computer system. One way for hackers to gain access to your computer system is through phishing, i.e., social engineering where the hacker sends a fraudulent email that appears to be a legitimate business email with links or attached files that, if accessed, release the ransomware on your computer system. Educating users on the types of social engineering scams being used and the importance of not clicking on links or opening files from untrusted sources are the first line of defense against a ransomware attack.

- **Ensure that your system software, including antivirus software, is regularly updated**
  Ransomware can be quite sophisticated, and may take advantage of weaknesses in your computer system's architecture. Ensuring that your operating system and programs are regularly updated with security patches can increase the efficacy of your computer system's built-in security. Likewise, having antivirus software is important for early detection; however, if it is not regularly updated, it will not be as effective at locating and isolating potential malware.

If available, employ Endpoint Detection and Response (EDR)

- An endpoint is any point in your computer system or network where communication occurs, i.e., entry and exit of data. EDR is a complementary component to antivirus software and offers a proactive tool for locating malware before it can negatively impact your computer system. However, EDR is not included in all antivirus platforms, and may require additional cost per user. Therefore, you must consider the cost and benefit of such an application. Depending on the size and volume of your agency, it may be a worthwhile investment in your business operation.

Automated Computer System Backup

- It is important that you backup your computer system daily. Why? Once your computer system is encrypted by ransomware, you are likely not going to be able to access that data without a key code from the hacker, which may be quite expensive and not guaranteed to get all of your data back. Moreover, even if the hacker provides a key that unlocks your data (after paying a hefty ransom), there is no guarantee that there is not more malware on your computer system that will activate at a later date. However, if your computer system is backed-up daily, you can simply wipe your system of the encrypted data and ransomware, and restore your data from the most recent backup (that predates the infection). Many cyber risk policies will cover that restoration cost up to the applicable sublimit for ransomware.

Continued

Create a Incident Response Plan

- Having an Incident Response Plan will provide your agency with a framework on how to respond to a cyber threat, such as a ransomware attack. It should include information on available resources, such as information regarding your Cyber Risk coverage, third-party vendors that are approved for servicing your computer system, and actions to take to avoid further damage from cyber threats.

Protecting your proprietary information and the PII of your customers is a necessary component of a trusted and successful business. Avoid being a victim to cyber extortionists by being proactive in the use and management of your computer system.

[1]A type of malware designed to encrypt a user's data and lock the user out of their system. Some types of ransomware allow for the exfiltration of data, while others merely restrict access to the data.
[2]Cyber Security Trends in 2021, Firch, Jason, MBA, published December 31, 2020
[3]This Year In Ransomware Payouts (2020 Edition), Soare, Bianca, published December 18, 2020

Utica National Insurance Group
Insurance that starts with you.®
Utica Mutual Insurance Company and its affiliated companies, New Hartford, NY 13413
www.uticanational.com • 1.800.598.8422

5-R-1388 Ed. 2-21