Ransomware Takes a Mega Bite

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE

Recent global cyber attacks have garnered a lot of attention. Ransomware is a type of malware that prevents or limits users' access to their computer systems, holding them hostage by either locking the screen or encrypting or otherwise disabling access to the data, until a ransom is paid.

We are well aware in the insurance industry that we have two distinct roles related to cyber. First, like any business or entity, we have a need to protect the information we hold. Second, we have a unique opportunity to help protect entities. Since ransomware is so prevalent, it is important that insurance companies understand the threats that exist for both their company and their customers.

Ransomware is a significant worldwide problem, and it is not new. While attacks have become increasingly more common since 2005, the first reported attack occurred in 1989, targeting the healthcare industry. In 2016, the rate of attacks increased threefold. A Kaspersky Labs report stated that, during the period from January to September 2016, attacks on businesses increased from one every two minutes to one every 40 seconds. Attacks on individuals occurred every 10 seconds. Looking at it a different way, 42 percent of small- to medium-sized businesses were victims in 2016.

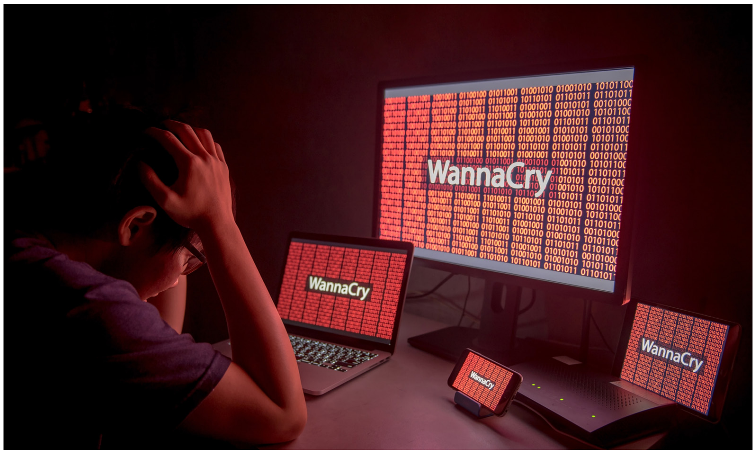
Ransomware is more than just a nuisance. It disrupts businesses in several ways. Potential threats include exposure of confidential information, loss of essential data, and loss of revenue due to inability to access systems.

There are two types of ransomware that exist. One encrypts the data. The other locks users out of their device(s). Victims receive a message telling them that they must pay a certain dollar amount in bitcoin within a specific time period. After that time period, the ransom may increase, or files may start being deleted. Bitcoin is used because the hackers can remain almost completely anonymous and the virtual currency allows them to be paid without any sort of money trail. Payment of the ransom is meant to provide a decryption key that enables the victim to unlock their system and regain access their data.

Paying the ransom does not mean that you will reclaim your data. Even after the ransomware is removed, there can still be a secondary malicious program residing on the system. Or, ransomware can scam a person or company out of the money and not restore the data or access to the data. Some ransomware is designed to delete data regardless of whether a ransom is paid.

Should a ransomware attack occur, it is important to turn off all devices and disconnect them from the network. Experts recommend that a ransom NOT be paid. Contact all users to alert them of the attack and inquire with each person to identify where the attack originated. This is done by pinpointing where and when the earliest evidence of the attack occurred. Reimaging infected devices will ensure that the ransomware is gone.

There are a number of steps that should be taken to reduce exposure to ransomware, starting with regular security updates and external backup of systems. Regular checks of the backup, testing the ability to restore the information, as well as knowing what is actually being backed up, are also essential preventative measures. The frequency of required backups will vary depending on the type of entity and data. A good antivirus and/or anti-malware program with regular—and preferably automatic—updates and scanning is



always recommended. Restoration of data from a backup should only be conducted on a new device or one that has been wiped clean to prevent reinfection.

Keeping systems updated is an essential step in protection from malicious attacks. In May 2017, WannaCry infected more than 230,000 computers in more than 150 countries. Hospitals in the United Kingdom were forced to cancel operations and divert ambulances. It is interesting to note that the vulnerability had been discovered, and a patch issued by Microsoft, two months prior to the May attack. Only those who had not installed the patch remained vulnerable.

As of mid-June 2017, 327 ransom payments totaling more than $132,000 had been made. Of course, as was outlined earlier the actual money paid is only the tip of the iceberg as far as the costs and overall ramifications of a ransomware attack.

Another similar attack occurred on June 27, 2017. Starting in the Ukraine, it impacted systems around the world. Multinational companies shut down operations to prevent spread of the attack. Some believe that the hacking tools used in these attacks were developed by and stolen from the National Security Administration (NSA), though this has not been confirmed.

While ransomware infection typically occurs as the results of downloading a file or opening an attachment to an e-mail, this is not always the case. WannaCry attacked computers without user intervention. The ransomware searches the internet for vulnerable computers running Microsoft operating systems.

Ransomware can disrupt operations and even destroy records of businesses and individuals. It is essential that insurance companies and their customers understand the risks, potential exposure, and ways to protect themselves from ransomware attacks. We know cyber security is an important aspect of any business or operation, but it is key to not view putting protections in place as a one time or once a year or even once a month exercise. Cyber crimes are evolving every day and hackers are becoming increasingly more sophisticated in their attacks. Companies need to remain informed and poised to act to stay as secure as possible. Insurance is one part of putting greater protections in place. The cyber security industry is understandably greatly expanding and thankfully working to keep up with the criminals who are behind the attacks. Sharing information has proven to be one of the most effective means of keeping pace with the crimes being committed.

Since cyber is one of the first risks that does not have geographic boundaries, it completely opens up how we approach protections and insurance. Risks were once localized, for example to one car or structure or sometimes a large swath of a state or country, but cyber has changed the entire dynamic, with even one event like WannaCry having consequences on a global scale.

This article originally appeared in the NYIA NY Connection Magazine.