The Rising Risk of Ransomware

I get a lot of questions regarding the hot topic of ransomware. While I am not aware of a Kentucky bank that has been affected, my contemporaries in other states tell me they have had client banks who have been. This is a timely article by a good friend. If you have questions regarding coverage and breach response services for these type of attacks, feel free to give me a shout.

Chuck Maggard, President & CEO
KenBanc/KBA Insurance Solutions
cmaggard@kybanks.com

by Craig M. Collins, OneBeacon Financial Services
& Joe Budzyn, OneBeacon Technology Insurance

Ransomware is the latest cyber extortion tool devised to threaten both businesses and individuals. Having affected financial institutions, hospitals and many other types of organizations, ransomware has been featured prominently in the news over the past few years. In 2015 alone, the Federal Bureau of Investigation (FBI) reported 2,400 ransomware-related complaints totaling a loss of more than $24 million. While some affected have paid the ransom and recovered their computer data, others have lost theirs forever.

What is ransomware, and how can banks protect themselves against this formidable risk?

How It Works: Similar to a virus, ransomware is malicious software that infects a computer. It can arrive via several mechanisms: a malicious email attachment, embedded in a malicious website download, attached to a phishing email, or even a web link that automatically downloads the ransomware when it is clicked.
Once a user's files and documents are encrypted, they become inaccessible until a ransom is paid. A user is instructed to pay ransom within a certain timeframe and through a method that is fairly convenient yet difficult to trace back to criminals. This may include wire transfers, pre-paid payment cards, Bitcoin or premium cost SMS services. While criminals say they will provide the user a decryption key necessary to recover their files, there is no guarantee that data will be recovered after the ransom is paid. Additionally, paying the ransom does not prevent future infection with the same or different ransomware and the cycle repeating.

Another type of ransomware locks a user's device to prevent its usage. The lock message often accuses the user of a crime and appears to come from a branch of law enforcement. The files may not be encrypted during this attack. If the lock screen ransomware is removed, the files are typically untouched.

The Damaging Impacts: While everyone is at risk for ransomware, banks are particularly attractive targets. Criminals recognize that financial institutions maintain a bevy of personally identifiable information and have the funds to pay a potentially lucrative ransom.

Beyond losing their files, banks that fall victim to ransomware can face monetary and business interruption losses, legal and IT service fees, lack of employee productivity and most importantly – compliance and reputational risks.

Mitigating Risks: The most effective defense against ransomware is prevention, and banks must take precautionary measures to protect themselves and their customers.

Back Up Data: An extremely important process is to back up important data daily. This backup should be offline and disconnected from the computer, as some versions of ransomware can encrypt data stored on network drives or in cloud services when they are connected to the infected computer. The recovery function of your backup/restore procedure should be tested regularly. Effectively backing up current data will leave banks less vulnerable to the threat of ransomware. Even if a computer is locked, a bank won't be forced to pay to recover its data.

Train Employees: Ransomware phishing attacks can come through in the form of an email with a malicious attachment or URL. It is important for employees to be vigilant of such attacks. To help raise security awareness, consider sending simulated phishing attacks to keep employees on their toes and help them recognize what a phishing attempt might look like. Advise employees not to click on links or open attachments or emails from those they do not regularly do business with.

Use Superior Security Technology: Even with proper training, employees may open an attachment or visit an infected site. That is why it is necessary for banks to take other standard security technology measures such as ensuring a firewall is in place. Anti-virus software should be used to detect and prevent infection, while web and email filtering software should be used to reduce exposure. It is important to apply security patches and regularly update all security software.

Segregate Access: Managing user access to data can lessen the risk of a successful ransomware attack. The number of employees with administrative access should be limited, and access should not be assigned unless absolutely necessary. Employees should only have access to the files or directories that are relevant to their job functions. Networks and data should be separated for each organizational unit.

In the Case of an Attack: Despite a bank's best efforts to protect against ransomware, an incident may still occur. If it does, both the FBI and the Federal Financial Institutions Examination Council (FFIEC) encourage ransomware victims to notify law enforcement immediately. Law enforcement officials, such as the

continued at the bottom of the following page