ABA Insurance Services
MEMBER OF GREAT AMERICAN INSURANCE GROUP

Safe Talk®
Loss Control Bulletin

What steps can your bank take to protect against ransomware attacks and email fraud?

While the threat of ransomware is nothing new, the alarming trends suggest that attacks are evolving to be more disruptive with payment demands more consequential than previously known. Well-publicized ransomware incidents have targeted entities across industries, from government organizations and school districts to privately held operations, hospital systems and financial institutions. Ransomware is no longer simply a nuisance; attacks are rendering businesses inoperable, significantly eroding public confidence, and costing businesses millions to remediate.

Ransomware attacks typically begin with a targeted email message containing malicious software. Once introduced, the malware spreads throughout the network, encrypting documents or files and rendering them inaccessible until a ransom is paid by the victim.

In the past, these attacks normally targeted specific documents or files. **Today, however, the attacks are creating havoc by infiltrating entire operating systems; deleting onsite backups; and exfiltrating sensitive data**, with threat actors threatening to publish confidential information if their demands are not met. As these criminals become more emboldened, they are seeking larger ransom payments, now easily reaching seven figures.

In one recent incident, **a bank was shut down for several days after numerous systems in its environment were attacked**, including its core operating system, online banking platform, and telephones. The extortionists demanded a ransom in excess of $1,000,000.

The increasing frequency of attacks has garnered the attention of the U.S. Treasury's Office of Foreign Assets Control. An advisory issued in October 2020 provides some background on attacks, identifies several known malicious actors, and suggests a risk-based compliance program to mitigate exposure. The advisory also warns victims can be fined if they pay ransom to groups that are under economic sanctions. A similar advisory was issued by the Financial Crimes Enforcement Network.

Big picture, experts suggest common-sense security measures are the best first step in protecting your institution, including:

- Training employees to recognize suspicious emails and attachments
- Keeping antivirus and anti-malware software up to date
- Ongoing, regularly scheduled offsite (cloud based) backups that are not connected to the networks being backed up
- Refining incident response and business continuity plans to reflect today's threat environment

On a more basic level, remind employees and customers to be even more vigilant with the increase in fraudulent schemes related to the pandemic. **The ideal environment has been created for fraudsters to take full advantage of the underlying stress and potential vulnerabilities with email communication increasing exponentially.** As phishing scams continue to be extremely prevalent and typically one of the most common initiation points for fraud, remind employees to:

- Remain vigilant and view emails with a suspicious eye, especially those with certain key words, such as "coronavirus" or "COVID-19" as fraudsters may use virus-related words to effectuate scams. The importance of training employees to identify phishing emails and social engineering tricks cannot be overstated.
- Rotate passwords and not duplicate passwords for multiple sites or online sources.
- Be mindful when using third-party sites or applications.
- If working from home, change the default passwords on home networks or WiFi routers, and do not share or allow family members to access any computers or handheld devices used for business purposes.

Continue to educate customers about the prevalence of phishing and social engineering. Do not assume they understand the risks; often, attacks target individuals or small businesses who may be more prone to divulging sensitive information.

There are emerging technology solutions available to help fortify your defenses against malware. A number of providers offer

Continued ⇨

solutions that monitor entry points and network workflow to detect threats. The tools capture and analyze big data across many channels and use machine learning to continuously refine their algorithms to predict and prevent both novel and known variants of malware. The detection and response capabilities work in real time and are significantly more effective in thwarting threats from ransomware and other novel malware than off-the-shelf antivirus software.

As the frequency and severity of ransomware attacks continue to increase, it is critical that institutions evaluate the security measures they have in place and implement/update security measures to keep a step ahead of potential threats.

Visit abais.com for more loss control information or to view this SafeTalk® online. To subscribe to SafeTalk, request reprints or if you have questions about this newsletter or articles, contact marketing@abais.com or 800-274-5222.

The claims scenario in this material is provided to illustrate a possible exposure faced by you or your clients. The facts of any situation which may actually arise, and the terms, conditions, exclusions, and limitations in any policy in effect at that time, are unique. Thus, no representation is made that any specific insurance coverage applies to the claims scenario. This information provides guidance and is not intended as a legal interpretation of any federal, state or local laws, rules or regulations. ABA Insurance Services Inc. ("ABAIS") does not warrant that all potential hazards or conditions have been evaluated or can be controlled. The liability of ABAIS and its affiliates is limited to the terms, limits and conditions of the insurance policies issued by ABAIS.