Is Your Bank Ready for a Ransomware Demand?

By Tim Henry, Vice President/Managing Agent, UBA

Ransomware attacks are very much in the news in 2021. Every organization should prepare in advance for the steps it must take should a ransomware event occur. While attacks against municipalities, educational facilities, healthcare organizations, the retail industry, and pipelines pepper the news, ransomware attacks have targeted community banks and will continue to do so in the future.

Ransomware is malware that employs encryption to hold data at ransom. Early on, ransom demands were relatively modest and victims were inclined to pay the demands to quickly return their companies to operational.

To counter the threat of ransomware demands, among other steps taken by organizations was to beef up backups to ensure that data truly could be restored in the event of a disaster, including a ransomware attack.

Ever opportunistic, fraudsters have shifted their focus to **managed service providers** (MSPs), which serve many clients at once, under the theory that if the fraudster can access one client, they can access many, many more. Another focus shift was to the **remote workforce** and their access tools with the presumed lower levels of security utilized.

Double extortion tactics and increased demands. Cybercriminals have amped up the stakes and now use a two-pronged extortion tactic: 1) locking up company data and systems; and 2) threatening to leak private and confidential data publicly unless the ransom is paid. A reported third prong being used by some extortionists is to send ransom demands to customers/users/third parties who would be hurt by the leaked data of the threatened organization.

Now it's not enough to simply turn one's back on a ransomware demand and rely on rock solid data backups to restore the bank's system to normal.

Impact on cyber insurance. To add to the problem, average ransomware payments have increased to $312,000 and reportedly, ransomware victims paid a total of $350 million in 2020. The huge dollars involved has resulted in higher cyber insurance premiums, higher deductibles, lower coverage limits, coverage restrictions, and in some cases, non-renewals.

Refer to your IT professionals for ransomware prevention. The best way to counteract ransomware attacks is to prevent them. Consult with your IT professionals and MSPs to tighten up your security measures.

Educate your users. Many attacks begin with a phishing email which looks legitimate but contains a malicious attachment or URL. Constant education of your employees is necessary in our click first, read later environment.

Department of Treasury Advisory. On October 1, 2020, the Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory **prohibiting the payment of ransom demands** to individuals on the OFAC Specialty Designated Nationals and Blocked Persons List (SDN List) and other specified persons and countries. Please see the advisory at https://home.treasury.gov for a complete list of prohibited parties.

Steps to take in the event of an attack. Both the FBI and the Federal Financial Institutions Examination Council (FFIEC) encourage ransomware victims to notify law enforcement immediately. In addition, the FFIEC recommends notifying your appropriate bank regulator and filing a Suspicious Activity Report, if appropriate.

Insurance Implications. Notice of a potential ransomware matter should be given to the bank's insurance company(ies) **immediately**. Typically, a breach coach will be assigned to your case to determine the appropriate steps to take to deal with the ransomware demand and associated potential breach. Not only does the carrier work with designated vendors with specific expertise in the type of breach the bank has incurred, but costs incurred by the bank without carrier approval are not necessarily covered by the insurer. Various coverages are available to mitigate the bank's expenses and the bank should review its exposures and the appropriate coverages / limits to purchase with its experienced insurance advisor.

Is Your Bank Ready for a Ransomware Demand?

By Tim Henry, Vice President/Managing Agent, UBA

United Bankers' Agency (UBA) offers cyber insurance to protect your community bank in the event of a security breach. Our community bank specific insurance solutions will ensure you have the right coverage in place. In addition, UBA provides a full suite of identity theft protection products for your customers from basic consultation restoration to web watcher, idINTEGRITY Scan. For more information or to schedule a consultation, go to www.ubb.com/insurance.