Ransomware Preparedness

Minimizing the Risk of Total Loss of Records

SUMMARY

Ransomware has become the most visible cyber threat to our nation's networks.

While financial institutions have implemented good cybersecurity practices, the rapid advancements in ransomware and its potentially devastating consequences require that every financial institution review and update its controls.

Ransomware can result in a sudden and unplanned suspension of critical core banking services, and payment of a ransom does not guarantee records can be restored in a timely fashion or even restored at all. In severe cases, this could result in the financial institution's failure.

The attached Ransomware Self-Assessment Tool (R-SAT) has 16 questions designed to help financial institutions reduce the risks of ransomware.

INCREASING RANSOMWARE THREAT

The losses and sophistication from attacks in recent years have increased significantly. Global criminal operations have developed and distributed advanced ransomware. One Russia-based cybercriminal organization is responsible for ransomware that has compromised hundreds of banks and financial institutions in over 40 countries.

Because cities and school districts are public entities, the attacks on dozens of them across the country are well known. But attacks on hundreds of private companies are not reported. One global cyber insurer recently reported that its United States customers had 775 ransomware incidents in 2019. This represented a 131% increase over 2018, and 11% of those incidents were financial institutions. This trend is expected to continue.

Ransomware variants are not only increasingly more sophisticated; some cyber criminals are now exfiltrating data in advance of encrypting the files. The owner of the data is then extorted to pay the ransom, or the data will be publicly posted. Some institutions have paid the ransom to keep their customer's data from being made public even when they could restore from backup. Furthermore, with several cybercriminals sanctioned by the Treasury's Office of Foreign Assets Control (OFAC), paying a ransom to one of these entities would be a crime that may risk violating OFAC regulations[1].

[1] OFAC Ransomware Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Ransomware Preparedness

Minimizing the Risk of Total Loss of Records

KEY CONTROLS TO IMPLEMENT

There is no single measure to prevent ransomware attacks. It requires strong adherence to fundamental cybersecurity controls. But some measures are very important: strong backup practices and the use of Multi-Factor Authentication (MFA).

An institution can fail at all measures to prevent ransomware, but if it has true off-line, immutable and restorable backups, it can usually restore customer services and minimize the risk of failure.

Compromising administrative access credentials (username and password) is a crucial step for criminals to deploy ransomware. Therefore, MFA should be used by all employees for administrative access. Additionally, bank information stored in a cloud environment (outside of the bank's firewall) should only be accessed with MFA.

RANSOMWARE SELF-ASSESSMENT TOOL

The attached Ransomware Self-Assessment Tool (R-SAT) is derived from earlier work by the Bankers Electronic Crimes Task Force (BECTF). The task force is composed of CEOs of U.S. community financial institutions, the United States Secret Service, state bank regulators, and other industry stakeholders. It uniquely addresses the needs of community financial institutions.

Resources:

CSBS/USSS/BECTF 2017 *Best Practices for Banks: Reducing the Risk of Ransomware*

US Secret Service guidance on Preparing for a Cyber Incident

DHS Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center released a joint Ransomware Guide.

Center for Internet Security (CIS) Primer on Ransomware.

FBI Public Service Announcement with updated information on the ransomware threat.

DHS Cybersecurity and Infrastructure Security Agency (CISA) Dridex Malware Alert.

FinCEN Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.

OFAC Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments