Ransomware: Lessons Learned by Banks That Suffered an Attack

Executive Summary

Ransomware continues to present a major threat to the financial sector. This method of attack used by bad actors has evolved from the basic encryption of data to now include variations utilizing double and triple extortion, as well as distributed denial of service attacks (DDoS). For the financial sector, ransomware is much more than a financial issue of paying a ransom or a fee to recover stolen data. Ransomware also represents an operational threat and, in some instances, a threat to the very survival of the institution. Ransomware continues to evolve and will present risks to the financial sector for the foreseeable future.

Multiple state banking departments across the country collaborated on a study of financial institutions that were actual victims of ransomware attacks. This study revealed lessons learned about protecting banks from ransomware, as well as measures impacted banks took based on their experiences. Key findings from that study, contained in this report, suggest that:

- Most victims identified in the study ultimately did not use the R-SAT as a tool to guide the mitigation of ransomware risks prior to the incident, but all victimized institutions began using it fully after the incident;
- Multi-factor authentication (MFA) can help to mitigate ransomware risk if properly configured and implemented; and
- Effective monitoring of "hyper-local," as well as traditional social media is necessary to manage misinformation and maintain consumer confidence.

Background

Multiple state banking departments across the United States collaborated to conduct a study of state-chartered banks and credit unions that were victims of ransomware attacks from January 1, 2019, through December 31, 2022. Findings from this study, which are summarized in this report, were used to inform an update of the Ransomware Self-Assessment Tool (R-SAT), Version 2.0. The R-SAT was first released in 2020 by the Conference of State Bank Supervisors (CSBS)[1] in collaboration with a national task force of bank CEOs (the Bankers Electronic Crimes Task Force),

[1] The Conference of State Bank Supervisors (CSBS) is the national organization of state banking and financial regulators. Representing a network of financial regulators in all 50 U.S. states and territories, CSBS supports state regulators in advancing the system of state financial supervision by promoting safety and soundness, consumer protection, and economic growth and fostering innovative, responsive supervision.

and the United States Secret Service. A copy of the R-SAT, Version 2.0 is available to all institutions.

In addition to incorporating anonymized findings from the study in the updated R-SAT, CSBS performed an administrative role in the development and distribution of this report. CSBS staff did not participate in the study and did not have access to any confidential supervisory information used to complete the study.

Although ransomware is a cyber event of relatively low frequency, it has an extremely high impact. It is common for a victimized financial institution to be dependent on "the honor of criminals" to restore bank records and operations and to potentially avoid failure. On a broader scale, local, regional, and even national economic stability could be undermined through the use of ransomware. For example, a ransomware attack against multiple financial institutions could disrupt confidence in community banking if a threat actor failed to provide valid decryption keys or if they published large amounts of stolen consumer information. Notably, failure to provide ransomware decryption keys has been observed with past events (e.g., NotPetya).

In light of the banking industry's increased focus on cybersecurity, the number of victimized banks nationally has been relatively low. Consequently, the findings of this study are more informal than academic. However, the Bankers Electronic Crimes Task Force concluded that the results of the study were important to share with the banking industry.

In addition to the principal findings from the study, there were also some notable actions taken by CEOs following ransomware incidents to reduce the risk of becoming a repeat victim. These lessons learned have been incorporated, along with other practices to keep pace with changing ransomware threats, into the R-SAT, Version 2.0.

Significant Findings

While there were several findings that represented "failures" to follow basic controls, there were three significant findings that only became apparent as the result of banks becoming victims of ransomware. The three findings are listed and discussed below:

1. **Completion and proper use of the R-SAT is important.**
2. **Properly configured and implemented Multi-Factor Authentication (MFA) makes a difference.**
3. **"Hyper-local" social media must be understood, identified, and managed.**

Completion and proper use of the R-SAT is important.

A majority of victims identified in the study had not completed or had only partially completed the R-SAT and, ultimately, did not use it as a tool to guide the mitigation of ransomware risks. However, the study found that all institutions that were victims began using it fully after the incident. Furthermore, bankers indicated a focus on the R-SAT from a compliance perspective and overreliance on third parties versus fully understanding their ransomware risk.

- Multiple bankers said they were over-confident in using a partially completed R-SAT because they utilize and annually update the FFIEC Cybersecurity Assessment Tool (CAT). Bankers also said they had been content with not completing, or only partially completing, the R-SAT if prior examinations and audit reports had indicated no criticisms related to cyber risks.

- Some institutions reported an over-reliance on third parties for cyber risk management rather than fully comprehending the issues of ransomware.

- Some bankers knew their R-SAT had not been completed thoroughly or that it was completed by personnel with insufficient knowledge or experience to credibly evaluate the process. It is important to avoid thinking of the R-SAT as just another regulatory compliance process versus using it to help evaluate the institution's risks and controls.

These observations are consistent with the fact that regulatory guidance typically trails real-time threats. Cyber threats move much faster than traditional risks to the banking industry and therefore require the continuous monitoring and management of associated risks prior to the issuance of relevant regulatory guidance. Special supplemental security considerations are needed by the industry to fill gaps until broader security approaches are updated by regulators and auditors. Ultimately, without accurate answers to security control questions, such as those contained in the R-SAT, it is impossible to identify gaps and effectively manage ransomware risks.

Properly configured and implemented multi-factor authentication (MFA) makes a difference. Multi-factor authentication (MFA) was one control that was consistently implemented at all institutions following a ransomware incident (if they were not already using it). MFA is a seemingly simple security feature; however, there are many variations and methods of implementation, each with their own strengths and weaknesses. Effective implementation and proper configuration of MFA is crucial for obtaining the expected benefits.

- It is important to recognize that MFA can and has been circumvented. It is not a panacea for other weak security practices. Additionally, poor implementation can provide an institution with a false sense of security. Like most security practices, MFA implementation requires careful analysis of the type of MFA to be used, features to be enabled, and where it will be used within an institution. There should be carefully documented decisions for <u>not</u> using MFA for such things as:

    - privileged access management (PAM) (e.g., domain administrative access, application administrative access, etc.),
    - access to any cloud-based services (e.g., mortgage origination or cloud-based email like Microsoft 365), and

    - additional critical areas identified in the R-SAT, Version 2.0.
- Implementation of MFA requires focused attention to recognize its most beneficial features, apply the most appropriate type of MFA, and understand where its application will be most effective. The updated R-SAT has been heavily expanded to address MFA. It is beyond the scope of this report to fully discuss MFA; however, the following resources are provided for learning more about its usage and implementation. These resources are primarily for practitioners that will be implementing or strengthening an entity's MFA controls.
    - Authentication and Access to Financial Institution Services and Systems (ffiec.gov)
    - Implementing Phishing-Resistant MFA (cisa.gov)
    - Implementing Number Matching in MFA Applications (cisa.gov)
    - CEG Enhancement Guide: Implementing Strong Authentication (cisa.gov)

    FIDO (Fast Identity Online) Authentication, which is based on public key cryptography, is related to MFA but is a relatively new concept to some in the banking industry. This enhanced authentication method provides more security than traditional password-based authentication and has a variety of potential applications across the institution where more secure authentication is required, such as online banking services. The use of FIDO is a growing trend in the banking industry and is also mentioned in the latest FFIEC guidance on authentication.

    - FIDO (Fast Identity Online) Explained Video - FIDO Alliance
    - SP 1800-17, Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers | CSRC (nist.gov)

"Hyper-local" social media must be understood, identified, and managed.

It is important that banks develop crisis communication procedures to identify and manage "hyper-local" social media platforms (e.g., Nextdoor, Facebook Neighborhoods, Citizen, and any other platforms used by your stakeholders), as well as "traditional" social network websites (e.g., Facebook, Instagram, X (f/k/a Twitter). A financial institution with multiple branches might need to address multiple "hyper-local" social media platforms.

- Once a problem surfaces (for example, if a customer cannot access their funds), the issue can rapidly accelerate to an uncontrollable state. It is critical to get in front of any misinformation, as some social media activity thrives on sensationalism. In the absence of information from the institution, it is reasonable to assume that the information void will be filled by someone outside of the institution, often without factual knowledge of the actual situation.

- Although the failure of Silicon Valley Bank was not related to ransomware, it demonstrated that social media, combined with the speed of electronic funds movement,

can quickly become a catalyst for panic among consumers. This immediately impacts customer confidence and can cause significant or even irreparable damage to brand reputation even after a ransomware incident is resolved.

Discussion of Additional Useful Findings:

In addition to the primary findings detailed above, the following important observations and findings were identified during the study:

- **Awareness of Cloud-Based Storage and Services:** The use of cloud storage and other cloud-based services is expanding rapidly. Knowing the location of the institution's data and whether it is protected at all times is crucial when utilizing cloud storage. This is true not only for data stored in the cloud, but also for any cloud-based services relied upon by your institution and your customers.

- **Changing Ransomware Tactics:** Ransomware has traditionally been used as leverage to obtain a payment, or "ransom," in exchange for decryption keys to restore encrypted data. However, some threat actors have also executed simultaneous DDoS (Distributed Denial of Service) attacks to exert more pressure on the institution to pay the ransom. More recently, criminal gangs have begun shifting to tactics known as "double extortion," and "triple extortion."

    a. Double extortion occurs when a financial institution's data is encrypted as well as stolen (exfiltrated). Although a financial institution may have good backups and the ability to restore data without the need for decryption keys, threat actors still demand payment of a ransom in exchange for their promise not to publicly publish the institution's stolen customer information.

    b. Triple extortion occurs when threat actors further threaten to not only publish the information of customers, but also directly contact the customers themselves. This is a tactic used to either disparage the reputation of the bank or to extort a fee directly from the customers in exchange for not publishing their data.

    c. Since encrypting data is a time-consuming process, some threat actors have begun foregoing the encryption of data and are instead relying solely on the threat of publishing stolen data to extort payment of ransoms.

- **Controversial Practices:** Some institutions have chosen to pay extortion fees in an effort to protect the confidential records of their customers. However, this practice does not relieve the institution of its obligation to notify customers and regulators of the theft of personally identifiable information (PII). In addition, the payment of ransoms introduces the risk of violating OFAC sanctions.

Even if the data stolen in a ransomware attack is not PII, payment of ransoms to criminal elements is a very controversial practice. Ransom payment increases the profitability of ransomware activities and perpetuates the cycle of attacks on the banking industry. Until it becomes a less profitable endeavor for criminals, ransomware attacks will continue for the foreseeable future.

Conclusion

Ransomware remains a significant threat for financial institutions around the world, requiring expenditures of time, resources, and money to defend against its impact. For the financial industry to become a less desirable target for ransomware threat actors, it is imperative that all institutions make it more difficult for criminals to profit from these tactics. To help achieve this goal, all financial institutions should establish robust policies and procedures that address fundamental controls necessary to reduce the impact of ransomware attacks. In addition, all financial institutions are encouraged to fully complete the R-SAT, Version2.0 implement and configure appropriate MFA solutions, and be prepared to address hyper-local and traditional social media postings during an incident. Finally, institutions are also strongly encouraged to carefully evaluate the broader consequences of paying any ransom to further reduce the attractiveness of ransomware as a tool for exploiting financial institutions.

This report has been issued by CSBS based on the collaborative effort of several state bank regulatory agencies and their outreach to their regulated institutions. CSBS staff did not participate in the study and did not have access to any confidential supervisory information used to complete the study.