Ransomware:

What You Need to Know to Protect Your Financial Institution

For decades, hackers motivated by lucrative payouts have been preventing victims from accessing their files until a sum of money is paid. A recent report from McAfee indicates that cyberattacks leveraging encryption and file-locking malware have significantly increased this year. With the recent increase in attacks, financial institutions (FIs) need to take the threat of ransomware seriously and enact extensive planning to prepare. This white paper aims to give you a deeper understanding of ransomware, provides best practices for you to consider, and suggests the Jack Henry & Associates, Inc.® solutions that can help you mitigate ransomware risks.

jack henry & ASSOCIATES INC.®

Contents

What is Ransomware?

Ransomware is a form of malicious software (malware) that encrypts a victim's systems or data files. The attackers then demand a payment (ransom) from the victim to restore access to the files — often by a certain deadline. According to the 2019 Data Breach Investigations Report by Verizon, ransomware is the second most prevalent use of malware, primarily because the cybercriminal is not forced to rely on stealing the data.

Practical Implications of Being Infected with Ransomware

What could happen if your FI falls victim to a ransomware attack?

In the first quarter of 2019, **ransomware attacks grew by 118%** according to a report by McAfee.

- You could experience catastrophic business impact.
  - Because of the encryption and loss of access to critical data during a ransomware incident, your services could be taken offline, bringing operations to a full stop and leaving you unable to serve your customers.
- You could experience a total loss of your computer systems.
  - Ransomware can be deployed by cybercriminals to encrypt high-value files on all servers and workstations at your FI.
  - On-site and sometimes off-site backup systems can be encrypted, defeating business continuity planning and data restoration options.
- Your customer's data could be exfiltrated.
  - Data could be sent outside your FI before the encryption event. It can be used as additional leverage to get your FI to pay the ransom and potentially inflict reputational harm.
  - When data exfiltration is combined with ransomware, it could be more difficult to detect due to loss of internal system agents which would normally be operating and detecting the event.
- Your FI's reputation could suffer.
  - Disruptions in service caused by ransomware could lead your customers to lose trust in the security of your FI.

According to the 2019 Data Breach Investigations Report by Verizon, **ransomware is the second most prevalent use of malware**.

- You could experience a long recovery and rebuild process.
  - Even if post-attack decryption becomes a viable option by paying the ransom to the cybercriminal, systems that were encrypted may not be able to be recovered to their original state. A full rebuild of all computers and networks could be necessary to restore services. This process could take days to weeks, depending on complexity.
- Your employees could be affected.
  - Several of your employees will need to work around the clock to restore and validate your data. Additionally, your employees' private information could be exposed, causing further exploitation to them directly. Employee retention could be affected if they don't trust your FI to keep their information secure.
- You could experience additional security issues.
  - Ransomware rarely strikes alone. Cybercriminals likely lurked on the system for a while before attacking. The exploitation of vulnerabilities usually results in more than one malware infection that precipitates the actual encryption of critical information. Your systems and data files will need to be scrubbed to eliminate any other infections.

What Can You do to Mitigate Ransomware Risk?

To combat and reduce the risk of your FI being compromised, you must have a layered, comprehensive approach to your information security and business processes so you can successfully recover. According to the Cybersecurity and Infrastructure Security Agency (CISA), the following questions highlight defensive steps you can take to prevent ransomware infection:

- **Backups**: Do we back up all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
- **Incident Response**: Do we have an incident response plan, and have we exercised it?
- **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
- **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
- **Staff Training**: Have we trained staff on cybersecurity best practices?
- **Account Protections**: Have we implemented multi-factor authentication and are we minimizing account privileges?
- **Vulnerability Scanning and Patching**: Have we implemented regular scans of our networks and systems? Do we have an automated patch management program?
- **Network Traffic Monitoring**: Are we monitoring the network traffic crossing the boundary of critical networks, including industrial control systems?
- **Application Whitelisting**: Do we allow only approved programs to run on our networks?

In addition to these items from CISA, Jack Henry also suggests:

- **Malware Sandboxing**: Are we analyzing files/emails that are allowed through our security systems for potential new threats? Can we detect a zero-day or targeted attack toward our FI?
- **Heuristic Analysis**: Are we able to analyze our customer and employee activity to detect abnormal activity?
- **Data Leakage**: Have we implemented systems and processes to help ensure that data leaving our organization can be detected or prevented?

Reviewing these questions regularly at your FI can help facilitate thoughtful exercises and planning that could reduce the risk of a catastrophic ransomware event.

Finally, as a reminder, the most common delivery mechanism for malware continues to be email phishing and spam. These emails include malicious attachments or links to malicious or compromised websites. When employees open attachments or click on links, they open the door for an infection that can quickly spread throughout your entire network. Consequently, the most effective deterrent to malware is frequent targeted employee training.

Help is Available from Jack Henry

Your FI can combat ransomware with the following solutions from Jack Henry:

Centurion Enterprise-Level Recovery™

While multiple layers of cyber defense are important to detect and prevent ransomware attacks, increasing backup resiliency is a critical element of ensuring recoverability in case a ransomware attack occurs. If backup systems can be reached by cybercriminals who have breached institutional networks and have been able to gather privileged credentials to your institutions' admin accounts, having an offsite backup service that cannot have backups encrypted, erased, or changed by any user on the organization's network is a critical service for business continuity and recovery.

Centurion Enterprise Continuity Planning (CELR) is a hosted backup solution that provides off-site, offline backups. These backups can only be erased by Centurion employees upon verified requests from authorized institution admins. This makes CELR an excellent choice to protect critical backups from cybercriminals' ability to encrypt or erase backups. As backups are a high-value target to cybercriminals in ransomware attacks, eliminated to prevent an institutional target from quickly rebuilding their infrastructure, this decoupling of privileges could prevent the ability of a cybercriminal to impact backups. While cloud-based backup offerings provide offsite backup capability, many of these offerings are fully modifiable by institutional administrators and could be compromised. CELR should be considered strongly as part of your total business continuity and disaster planning.

Gladiator CoreDEFENSE Managed Security Services™

Gladiator's 24x7x365 Managed Security Services protect FIs' mission-critical IT solutions and critical data. These comprehensive services that include around-the-clock management, correlation, and monitoring of multiple security layers are specifically designed and developed for FIs to safeguard information assets, IT infrastructures, and business continuity by identifying and addressing internal and external security breaches.

Gladiator Business Continuity Planning™

Gladiator Business Continuity Planning helps FIs systematically restore their operational infrastructures in the event of temporary business interruptions or catastrophic disasters. These multi-tiered consulting services generate fully customized, enterprise-wide business continuity plans that identify and document mission-critical business functions and establish the procedures and testing required to restore each function's operations. These comprehensive plans facilitate the restoration of FIs' core and complementary solutions, leverage a proven best practices methodology, and help ensure compliance with the related regulatory requirements. Ongoing plan maintenance and mock disaster recovery services are also available. These services are provided by professional consultants with the expertise necessary to proactively prepare for disasters, expedite the resumption of FI operations, and minimize customer impact and inconvenience.

SecurePort, a Sheltered Harbor® Solution

SecurePort, a Sheltered Harbor Solution is Jack Henry's data vaulting solution built from the standards and procedures of the Sheltered Harbor organization. Sheltered Harbor is a not-for-profit industry-led initiative under the Financial Services Information Sharing and Analysis Center (FS-ISAC) umbrella dedicated to enhancing financial sector stability and resiliency. Jack Henry has been at the forefront, devoting resources and leadership to support this important initiative designed to protect consumers, and public confidence in the financial system, if a cataclysmic event like a cyber-attack causes critical systems – including backups – to fail. SecurePort provides a data vaulting solution that transfers the FI's critical data, which includes deposit account records, customer records, customer-account records, holds records and sweeps records, into a secure data vault storage solution. The data vault is encrypted, unchangeable, and completely separated from the institution's infrastructure (air-gapped), including all backups. SecurePort launches in early 2020 for SilverLake System® core clients that are Sheltered Harbor compliant, with remaining Jack Henry core platforms to follow for SilverLake System core clients that are Sheltered Harbor compliant. While Sheltered Harbor is currently building the requirements and standards around restoration, at this time the solution does not provide comprehensive recovery of a bank's core systems or business processes. Jack Henry will research the restoration piece of Sheltered Harbor when the standards are published.

Summary

Improper management of the risks associated with a ransomware infection can be devastating and costly to your organization. Awareness and education are key to protecting against ransomware attacks. By educating yourself and your users on basic protection practices and keeping up with current security threats, you can mitigate the risk of ransomware and keep your data safe.

Please reach out to Jack Henry should you need assistance with guarding against this risk.