Ransomware Self-Assessment Tool (R-SAT)

October 24, 2023
Version 2.0

Developed in collaboration with the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service

Purpose

The Bankers Electronic Crimes Taskforce (BECTF), state bank regulators, and the United States Secret Service collaborated to develop this tool to help financial institutions periodically assess their efforts to mitigate risks associated with ransomware[1] and identify gaps for increasing security. This document provides executive management and the board of directors with an overview of the institution's preparedness towards identifying, protecting, detecting, responding, and recovering from a ransomware attack. It may also assist other third parties (such as auditors, security consultants and regulators) that might review your institution's security practices.

Ransomware is a type of malicious software (malware) that encrypts data on a computer, making it difficult or impossible to recover. Attackers usually offer to provide a decryption key after a ransom is paid; however, these keys may not work (if they are provided at all), which could make the financial institution's critical records unavailable. In addition, attackers may utilize extortion tactics to threaten the institution with public disclosure of exfiltrated customer or company information if the ransom is not paid. However, financial institutions choosing to pay ransoms, as well as companies that facilitate ransom payments to cyber actors on behalf of victims, including cyber insurance firms and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but may also violate OFAC regulations.[2]

Completing the Ransomware Self-Assessment Tool (R-SAT)

The R-SAT is derived from the BECTF's *Best Practices for Banks: Reducing the Risk of Ransomware.*[3] Those best practices have been updated in the R-SAT to address today's environment. Due to the sophistication of ransomware, some areas in the R-SAT are mildly technical. You may wish to ask your institution's vendors and third-party service providers to complete some questions. Finally, due to the potential sensitivity of information contained in the R-SAT, institutions are cautioned to exercise due care to protect against unauthorized access or disclosure of the completed document outside of the institution.

Preparer Information

Please provide the following information regarding the preparer of this document.

Name and Title:	**Email and Phone Number:**
Institution Name:	**Date Completed:**
Date Reviewed by Board:	

[1] Refer to Federal Financial Institutions Examination Council (FFIEC) Joint Statement: Cyber Attacks Involving Extortion

[2] Refer to FinCEN Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments and OFAC Ransomware Advisory

[3] Refer to Best Practices for Banks: Reducing the Risk of Ransomware (csbs.org)

IDENTIFY/PROTECT	
1. Has the institution implemented a comprehensive set of controls designed to mitigate cyber-attacks (e.g., FFIEC CAT, CIS Critical Security Controls, NIST Cybersecurity Framework)? If so, what standard(s) or framework(s) (if any) are used to guide cybersecurity control implementation?[4] *Check all that apply.* *Note: State bank regulators do not endorse any specific standard or framework.*[5]	☐ YES ☐ NO ☐ AICPA SOC ☐ CIS Critical Security Controls ☐ COBIT ☐ CRI Profile ☐ FFIEC CAT ☐ International Organization for Standardization (ISO) ☐ NIST Cybersecurity Framework ☐ PCI DSS ☐ Other Describe.
2. Has a gap analysis been performed to identify controls that have not been implemented but are recommended in the standards and frameworks that the institution uses? If yes, has the gap analysis been reviewed by the board, senior management, and, if applicable, the technology committee?	☐ YES ☐ NO ☐ YES ☐ NO

[4] American Institute of CPAs System and Organization Controls (AICPA SOC); Center for Internet Security (CIS) Critical Security Controls; Control Objectives for Information Technologies (COBIT); Cyber Risk Institute (CRI) Profile; Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT); International Organization for Standardization (ISO); National Institute of Standards and Technology (NIST) Cybersecurity Framework; and Payment Card Industry Data Security Standard (PCI DSS)

[5] Refer to FFIEC Press Release: FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness

IDENTIFY/PROTECT	
3. Does the institution have a cyber insurance[6] policy(s) that includes ransomware coverage? If yes, please provide the name of the insurer(s). Provide the name of the insurer(s).	☐ YES ☐ NO
If yes, does the policy(s) collectively provide any of the following services? *Check all that apply.*	☐ Data retention services ☐ Breach response ☐ Cyber extortion assistance ☐ Data loss (hardware replacement) ☐ Third-party coverage ☐ Regulatory penalties assistance ☐ Legal expenses ☐ Forensic services ☐ Negotiating/facilitating ransom payments ☐ Customer notification assistance ☐ Customer call center services ☐ Management of public relations ☐ Customer credit monitoring

[6] Refer to FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs

IDENTIFY/PROTECT

4. Indicate if the following systems or activities are processed or performed internally, are outsourced to a third party, such as vendors that specialize in core services or provide network administration (a/k/a managed service providers (MSPs)), or a combination of the two. In addition, please identify any services that are based in a cloud environment. *Check all that apply*.

	Cloud-Based	In-House	Outsourced
Core Processing	☐	☐	☐
Network Administration	☐	☐	☐
Email Service	☐	☐	☐
File Imaging (Checks, Loans, etc.)	☐	☐	☐
Trust Services	☐	☐	☐
Mortgage Loans	☐	☐	☐
Investments (Bonds, Stocks, etc.)	☐	☐	☐
Other Critical Services * *(Please list below):*			
Other critical services.	☐	☐	☐
Other critical services.	☐	☐	☐
Other critical services.	☐	☐	☐
Other critical services.	☐	☐	☐
Other critical services.	☐	☐	☐

* Services such as data storage, wire transfer, payroll systems, general ledger, other customer facing applications, etc.

IDENTIFY/PROTECT	
5. Is any of the data identified in the previous question housed in a location(s) outside of the United States?	☐ YES ☐ NO
If yes, has management discussed any applicable privacy regulations in those foreign jurisdictions, such as GDPR, PIPEDA, etc.?[7]	☐ YES ☐ NO
6. Do any third-party vendors (including any MSPs) have continuous or intermittent remote access to the network?	☐ YES ☐ NO
If yes, explain the different types of access methods used, such as remote scripting, screen sharing, VPN, etc. If yes, explain the different types. If yes, do <u>all</u> of these vendors implement controls to prevent ransomware and threat actors from moving from their network to the institution's network via the access methods noted above? ☐ YES ☐ NO	
Describe applicable vendor-implemented controls below. In addition, identify below which vendors <u>do not</u> have such controls in place. Describe applicable vendor-implemented controls and identify vendors that do not have controls in place. As part of the institution's vendor management process, do all third-party vendors with remote access to the network provide, at least annually, an independent audit that confirms these controls are in place? ☐ YES ☐ NO	
7. Do risk assessments include ransomware and extortion as a threat?	☐ YES ☐ NO
If yes, are common potential attack vectors, such as phishing, watering holes, malicious ads, third-party apps, attached files, and unpatched vulnerabilities, identified?	☐ YES ☐ NO

[7] Examples of international privacy laws include General Data Protection Regulation (GDPR), which covers data protection and privacy in the EU and the EEA, and the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs data privacy in Canada.

IDENTIFY/PROTECT

8. Have all ransomware risks and threats identified in risk assessments been appropriately remedied or mitigated to an acceptable risk level? If no, identify any unmitigated risks below. Identify any unmitigated risks.	☐ YES ☐ NO
9. Are all employees periodically provided information on emerging ransomware threats via branch meetings, emails from IT security personnel, etc.?	☐ YES ☐ NO

10. At what frequency is formal employee security awareness training (classroom training, web-based training, self-paced learning, etc.) provided to employees?

- ☐ Annually
- ☐ Semi-annually
- ☐ Quarterly
- ☐ Monthly
- ☐ Other Describe other.

Indicate which of the following, if any, are included as part of employee security awareness training programs. *Check all that apply.*

- ☐ Social engineering and phishing testing
- ☐ Ransomware and extortion
- ☐ Incident identification and reporting
- ☐ Acceptable use policy training and written employee acknowledgement

IDENTIFY/PROTECT

11. Does the institution perform phishing test exercises (at least quarterly) to measure employee vigilance and awareness of phishing threats?	☐ YES ☐ NO
If yes, are metrics from phishing test exercises used by management to evaluate training effectiveness and guide additional employee training efforts?	☐ YES ☐ NO

12. Which of the following controls have been implemented for backing up data for core processing, network administration, and other critical services? Check all that apply and provide explanations where needed in the comment box below. Use the blank columns to identify controls for backing up data for other critical services, such as trust services, mortgage loans, investments, image files, email services, and others; additional columns are also provided in Appendix A, if needed. For services managed by an outside vendor, consider asking the vendor to complete the questions, if necessary.

Controls	Core Processing	Network Admin	Enter Data Type	Enter Data Type	Enter Data Typ
a) Procedures are in place to prevent backups from being affected by ransomware and extortion. *Describe procedures below.*	☐	☐	☐	☐	☐
b) Access to backups requires an authentication method(s) that differs from the network method of authentication. *If not, describe authentication below.*	☐	☐	☐	☐	☐
c) At least daily full system (vs incremental) backups are made. *If not, describe below.*	☐	☐	☐	☐	☐
d) At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.), and they are stored separately. *Describe practices below.*	☐	☐	☐	☐	☐

IDENTIFY/PROTECT					
Controls	**Core Processing**	**Network Admin**	Enter Data Type	Enter Data Type	Enter Data Typ
e) At least one backup is offline (air gapped) and/or immutable. *Provide additional details below.*	☐	☐	☐	☐	☐
f) Procedures are in place to allow immediate off-network restoration (i.e., cold site, warm site, hot site) of backups to facilitate continuity of essential operations (teller platform systems, etc.) while network systems are offline, being cleared, and/or reimaged following an incident. *Provide additional details below.*	☐	☐	☐	☐	☐
g) Backup testing is conducted at least annually to help ensure the institution can recover from ransomware using an unaffected backup. *Describe testing frequency below.*	☐	☐	☐	☐	☐
h) Procedures are in place to validate the sterility of data backups prior to restoration to prevent reinfection. *Provide additional details below.*	☐	☐	☐	☐	☐

IDENTIFY/PROTECT

Describe backup controls.

a.) Describe backup controls.

b.) Describe backup controls.

c.) Describe backup controls.

d.) Describe backup controls.

e.) Describe backup controls.

f.) Describe backup controls.

g.) Describe backup controls.

h.) Describe backup controls.

IDENTIFY/PROTECT

13. Has multi-factor authentication (MFA) been implemented in the institution? ☐ YES ☐ NO

If yes, does the institution rely on stronger application-based or phishing-resistant authentication methods, as opposed to weaker SMS or voice-based authentication? [8] Examples of stronger authentication methods include authentication via mobile push notification (with or without number matching); one-time passwords; token-based one-time passwords or, ideally, phishing resistant MFA such as FIDO/WebAuthn authentication or public key infrastructure (PKI)-based authentication.

☐ YES ☐ NO

Please indicate where/how MFA is used. *Check all that apply.*

- ☐ For privileged access management (PAM) (domain administrative access, application administrative access, etc.)
- ☐ By all users that access any cloud-based service (mortgage origination, HR platforms, etc.)
- ☐ For cloud email services, such as Microsoft 365 and others
- ☐ For access to external applications hosting non-public information (NPI)
- ☐ For VPN/Remote Desktop (RDP) access into the network
- ☐ For vendor access into the network
- ☐ For internal service accounts
- ☐ For customers accessing NPI (eBanking services, remote deposit capture, etc.)
- ☐ Other:

Describe other area(s).

If there are any specific areas the institution has identified where the implementation of MFA is not planned or has been deferred to a later date, please identify below.

Identify any specific areas where the implementation of MFA is not planned or has been deferred to a later date.

[8] Not all forms of MFA provide the same level of protection. Refer to CISA's Implementing Phishing-Resistant MFA for additional details on the strengths and weaknesses of various types of MFA.

IDENTIFY/PROTECT

14. Indicate which of the following additional preventative controls have been implemented. *Check all that apply.*

- ☐ Have implemented change management and patch management procedures that facilitate the prompt installation of critical patches and firmware updates
- ☐ Have disabled Remote Desktop Protocol (RDP) or it must be accessed from behind a firewall, through a VPN configured for network-level authentication, and/or the IP addresses of all authorized connections are on a whitelist/allow list
- ☐ Have eliminated administrative access to endpoints, workstations, and network resources for all but network support personnel
- ☐ Have implemented technical and administrative controls to manage the use of removeable media, such as USB drives, portable hard drives, etc.
- ☐ Have implemented configuration procedures to change default settings, user accounts, and passwords for hardware and software.
- ☐ Have adopted "least privileged access" concept for granting users access to shared folders and other resources
- ☐ Have established a process for provisioning and reviewing Active Directory access, especially for service accounts, and the process is actively managed and reported to management
- ☐ Have implemented procedures governing the resetting or replacement of authentication credentials for users
- ☐ Have implemented a jump box (a/k/a bastion host) or administrative VLAN for segregating administrative/privileged access to sensitive servers and data.
- ☐ Have disabled all unnecessary browser or email client plugins
- ☐ Have implemented a domain-based message authentication, reporting, and conformance (DMARC) policy and set to at least quarantine status
- ☐ Have maintained and enforced network-based URL and DNS filtering
- ☐ Have intrusion detection systems (IDS) and intrusion prevention systems (IPS) that detect and block ransomware activity, including the exchange of encryption keys
- ☐ Have implemented network segmentation and/or micro-segmentation to prevent the spread of ransomware and the movement of threat actors across the entire network
- ☐ Have implemented behavior-based malware prevention tool(s)

Describe behavior-based malware prevention tools.

IDENTIFY/PROTECT	
15. Are ransomware scenarios specifically included as part of annual testing of the Incident Response Plan?	☐ YES ☐ NO
Does executive management participate in annual testing of the Incident Response Plan?	☐ YES ☐ NO
Do appropriate C-suite representatives actively participate in annual testing of the Incident Response Plan?	☐ YES ☐ NO

DETECT

16. Indicate which of the following monitoring practices are utilized for servers, backup systems, workstations, networks, and other endpoints. *Check all that apply.*

- ☐ Data Loss Prevention Program that prevents large amounts of data from being exfiltrated by any method or protocol without the use of multi-factor authentication AND without providing real-time alerts to a monitored endpoint
- ☐ Blocking and alerts of executable files attempting to connect to the Internet
- ☐ Alerts to changes in privileged access rights
- ☐ Active monitoring of network management tools used on workstations, such as Windows Management Instrumentation (WMI), PsExec, and other power shell scripts
- ☐ Detection of suspicious file extensions
- ☐ Detection of large amounts of file renaming
- ☐ None of the above.

RESPOND

17. Does the Incident Response Plan identify a person (internal or third-party) with the expertise to manage/coordinate all aspects of a ransomware response?	☐ YES ☐ NO

18. Indicate which of the following ransomware response procedures are included in the Incident Response Plan. *Check all that apply.*

- ☐ Designate an individual to monitor social media and news sources for public awareness and discussions of the incident. All social media platforms should be monitored, including "hyper-local" platforms such as Nextdoor, Facebook Neighborhoods, Citizen, and others used in your community(s). Active accounts should be maintained to allow rapid posting, as necessary, and reading of any relevant information.
- ☐ Prevent or isolate the ransomware from spreading to other systems.
- ☐ Notify incident response stakeholders.
- ☐ Immediately contact federal law enforcement. Federal law enforcement agencies, such as the US Secret Service and FBI, have subpoena powers to access logs and other critical information quickly, possess knowledge of threat actor behaviors and ransomware variants, and may have access to decryption keys.
- ☐ Grant authority to a specific individual(s) to shut down a third party's access to the network.
- ☐ Implement "out-of-band" communications procedures to mitigate potential threat actor use of single sign-on (SSO) to access containment and remediation efforts.
- ☐ Mitigate all exploited vulnerabilities.
- ☐ Perform threat hunting to minimize back-door risks.
- ☐ Immediately notify legal counsel, as well as cyber insurance company, if applicable.
- ☐ Implement alternative strategies for connecting to critical third-party vendors in the event of an infection.
- ☐ Determine the scope of the infection by hiring specialized third parties or, if appropriately experienced, by using in-house or MSP resources.
- ☐ Establish escalation processes for enacting the Business Continuity/Disaster Recovery Plan in the event of significant and/or long-term impacts to bank operations.

RESPOND

- ☐ Discuss any prospect of ransom payment with the board and any appropriate committee(s) prior to payment, including awareness of and compliance with OFAC guidance.
- ☐ Establish procedures to ensure forensic information and audit logs are preserved before any restoration is performed.
- ☐ Restore systems/data if necessary.
- ☐ Contact federal regulators within 36 hours and state regulators in accordance with applicable state requirements.
- ☐ Prepare communications document for internal staff to use when responding to customer questions.
- ☐ Determine the cause of the incident.
- ☐ Periodically update contact information for firms that assist with incident response.
- ☐ Notify all affected employees, customers, and/or vendors as warranted.
- ☐ Notify and periodically brief incident stakeholders as appropriate (employees, board, stockholders).
- ☐ Other (please list below)

Describe other ransomware response procedures.

RESPOND

19. Has the institution identified any third parties to be engaged in the event of a successful ransomware or extortion attack? ☐ YES ☐ NO

If yes, do prearranged service contracts or, at a minimum, contact information exist so that legal and contract issues do not delay the institution's response? ☐ YES ☐ NO

If yes, do you or do you require these third parties, including cyber insurance companies, to promptly engage with law enforcement? ☐ YES ☐ NO

Are any such third parties pre-approved by the bank's cyber insurance provider? ☐ YES ☐ NO

RECOVER

20. Which of the following are included in procedures for returning to normal operations? *Check all that apply.*

- ☐ User testing after restoration
- ☐ After action review to identify lessons learned
- ☐ Updating the Incident Response Plan with lessons learned
- ☐ Providing refresher training, as necessary, to employee(s)
- ☐ Notifying stakeholders as appropriate (employees, board, stockholders)
- ☐ Other (Please list below)

Describe other procedure for returning to normal operations.

COMMENTS (Optional)

Comments (Optional)

APPENDIX A

IDENTIFY / PROTECT

Controls for Data Backup

Use the blank columns below to identify controls for backing up data for other critical services, such as trust services, mortgage loans, mortgage underwriting, mortgage support services, electronic funds transfer, securities and investments, image files, email services, data storage, general ledger, and other services not listed in **Question 12**. For data managed by an outside vendor, consider asking the vendor to complete the questions, if necessary. This Appendix may be duplicated if necessary.

Controls	Insert Data Type	Insert Data Type	Insert Data Type	Insert Data Type	Insert Data Type
a) Procedures are in place to prevent backups from being affected by ransomware. *Describe procedures below.*	☐	☐	☐	☐	☐
b) Access to backups requires an authentication method(s) that differs from the network method of authentication. *If not, describe authentication below.*	☐	☐	☐	☐	☐
c) At least daily full system (vs incremental) backups are made. *If not, describe below.*	☐	☐	☐	☐	☐
d) At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.), and they are stored separately. *Describe practices below.*	☐	☐	☐	☐	☐

Controls Continued	Insert Data Type	Insert Data Type	Insert Data Type	Insert Data Type	Insert Data Type
e) At least one backup is offline (air gapped) and immutable. *Provide additional details below.*	☐	☐	☐	☐	☐
f) Procedures are in place to allow immediate off-network restoration (i.e., cold site, warm site, hot site) of backups to facilitate continuity of essential operations (teller platform systems, etc.) while network systems are offline, being cleared, and/or reimaged following an incident. *Provide additional details below.*	☐	☐	☐	☐	☐
g) Backup testing is conducted at least annually to help ensure the institution can recover from ransomware using an unaffected backup. *Describe testing frequency below.*	☐	☐	☐	☐	☐
h) Procedures are in place to validate the sterility of data backups prior to restoration to prevent reinfection. *Provide additional details below.*	☐	☐	☐	☐	☐

APPENDIX A
IDENTIFY / PROTECT

Controls for Data Backup

Describe backup controls.

a.) Describe backup controls.

b.) Describe backup controls.

c.) Describe backup controls.

d.) Describe backup controls.

e.) Describe backup controls.

f.) Describe backup controls.

g.) Describe backup controls.

h.) Describe backup controls.

APPENDIX B

Ransomware Resources

In November 2022, The Federal Financial Institutions Examination Council (FFIEC) issued an update to the October 2018 Cybersecurity Resource Guide for Financial Institutions. The programs and initiatives in the guide are designed for, or otherwise available to, financial institutions. This resource and others listed below are actionable and can help financial institutions meet their control objectives and prepare to respond to cyber incidents.

FFIEC Cybersecurity Resource Guide: Cybersecurity Resource Guide for Financial Institutions, September 2022 (Revised November 2022) (ffiec.gov).

CISA Cyber Security Evaluation Tool (CSET): Ransomware Readiness Assessment (RRA): https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

CISA Stop Ransomware Resource Site: https://www.cisa.gov/stopransomware

Conference of State Bank Supervisors (CSBS) Ransomware Self-Assessment Tool: https://www.csbs.org/ransomware-self-assessment-tool