Nonbank Ransomware Self-Assessment Tool (Nonbank R-SAT)

October 15, 2024
Version 2.0

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

Adapted for nonbank institutions by the Conference of State Bank Supervisors

Purpose

The Nonbank Ransomware Self-Assessment Tool (Nonbank R-SAT), Version 2.0, was derived from the updated R-SAT, Version 2.0 for Banks, which was developed by CSBS, in collaboration with the Bankers Electronic Crimes Task Force (BECTF), state regulators, and the US Secret Service, to protect the banking industry. However, it contains important controls that companies of all types should use to assess their efforts to mitigate risks associated with ransomware[1] and identify gaps for increasing security.

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 company's critical records unavailable. In addition, attackers may utilize extortion tactics to threaten the company with public disclosure of exfiltrated customer or company information if the ransom is not paid. However, companies 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 Nonbank R-SAT

The Nonbank R-SAT is based on the BECTF's *Best Practices for Banks: Reducing the Risk of Ransomware*[3], and is aligned with many of the information security program requirements found in the Federal Trade Commission's Safeguards Rule.[4] Those best practices have been updated in the Nonbank R-SAT to address today's environment. Due to the sophistication of ransomware, some areas in the Nonbank R-SAT are mildly technical. You may wish to ask your company's vendors and third-party service providers to complete some questions. Finally, due to the potential sensitivity of information contained in the Nonbank R-SAT, companies are cautioned to exercise due care to protect against unauthorized access or disclosure of the completed document outside of the company.

Preparer Information

Name and Title:	**Email and Phone Number:**
Company Name:	**Date Completed:**
Date Reviewed by Board (if applicable):	

[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)

[4] Refer to Federal Trade Commission's Safeguards Rule.

IDENTIFY/PROTECT	
1. Has the company 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?[5] *Check all that apply.* *Note: State bank regulators do not endorse any specific standard or framework.*[6]	☐ YES ☐ NO ☐ AICPA SOC ☐ CIS Critical Security Controls ☐ COBIT ☐ CRI Profile ☐ FFIEC CAT ☐ International Organization for Standardization (ISO) ☐ NIST Cybersecurity Framework ☐ PCI Data Security Standard (DSS) ☐ Other (specify below)
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 company uses? If yes, has the gap analysis been reviewed by senior management and, as applicable, the board and the technology committee?	☐ YES ☐ NO ☐ YES ☐ NO

[5] 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)

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

IDENTIFY/PROTECT

3. Does the company have a cyber insurance[7] policy(s) that includes ransomware coverage? If yes, please provide the name of the insurer(s) in the box below.	☐ YES ☐ NO
If yes, does the policy(s) collectively provide any of the following services? *Check all that apply.*	☐ Data preservation consultation[8] ☐ 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

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

[8] As remediation activities are performed immediately following an incident, unintended consequences might occur (for example, if drives are wiped without imaging or valuable log data is deleted, etc.). This consideration is intended to help companies, particularly those smaller institutions with limited internal technical resources, understand whether the insurance company (via the breach coach and/or engaged supporting teams) might assist or consult with the company's IT teams regarding the preservation of data artifacts needed to enable appropriate forensic analysis of affected company systems.

IDENTIFY/PROTECT

4. Indicate which critical systems or activities your company (a.) processes or performs internally; (b.) outsources to a third party, such as vendors that specialize in core services or provide network administration (a/k/a managed service providers (MSPs)); or (c.) processes or performs through a combination both in-house and outsourced management. In addition, please identify any of these services that are based in a cloud environment. **Examples might include email services; network administration services; BSA/AML services; wire transfer services; e-commerce applications; fraud modeling or credit verification services; file imaging, loan servicing or origination software; any services for the processing, transmission, or storage of critical data; customer relationship management (CRM) software; or any other critical system or activity that might be unique to your company.** *Identify and check all that apply.*

	In-House	Outsourced	Cloud-Based
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐

IDENTIFY/PROTECT	
5. Is any of the data identified in the previous question housed in a location(s) outside of the United States? If yes, has management discussed any applicable privacy regulations in those foreign jurisdictions, such as GDPR, PIPEDA, etc.?[9]	☐ YES ☐ NO ☐ YES ☐ NO
6. Do any third-party vendors (including any service providers) 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, virtual private network (VPN) etc.

If yes, do <u>all</u> of these vendors implement controls to prevent ransomware and threat actors from moving from their network to the company's network via the access methods noted above?

☐ YES ☐ NO

If yes, describe applicable vendor-implemented controls below. In addition, identify below which vendors <u>do not</u> have such controls in place.

If yes, as part of the company'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

[9] 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	
7. Do your company's risk assessments include ransomware and extortion as a threat? 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 ☐ YES ☐ NO
8. Have all ransomware risks and threats identified in these risk assessments been appropriately remedied or mitigated to an acceptable risk level? If no, identify any unmitigated risks and the reasons why below.	☐ YES ☐ NO
9. Are all employees periodically provided information on emerging ransomware threats via branch meetings, emails from IT security personnel, training, bulletins, etc.?	☐ YES ☐ NO

IDENTIFY/PROTECT

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 (specify here) ☐

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

11. Does the company perform phishing test exercises on at least a quarterly basis 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

IDENTIFY/PROTECT

12. Which of the following controls have been implemented for backing up data for critical systems and activities? Use the blank column headers to identify these critical services and activities previously identified in Question 4, then check all that apply and provide explanations where needed in the comment box below. For systems data managed by an outside vendor, consider asking the vendor to complete the questions, if necessary. Additional columns are also provided in Appendix A, if needed.

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 any authentication process in place below.*	☐	☐	☐	☐
c) At least daily full system (vs incremental) backups are made. *If not, describe any backup process in place 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				
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 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 company 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.*	☐	☐	☐	☐

Describe backups here.

a.)

b.)

c.)

d.)

e.)

f.)

g.)

h.)

IDENTIFY/PROTECT

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

If yes, does the company rely on stronger application-based or phishing-resistant authentication methods, as opposed to weaker text message (SMS) or voice-based authentication? [10] 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 any customers accessing NPI
- ☐ Other (specify here):

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

[10] 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 required that it only 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 tools below)

IDENTIFY/PROTECT

15. Does the company have a written Incident Response Plan?[11]	☐ YES ☐ NO
If yes, is the Incident Response Plan tested at least annually?	☐ YES ☐ NO
If yes, are ransomware scenarios included as part of testing?	☐ 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.

[11] The Federal Trade Commission's Safeguards Rule does not require a written Incident Response Plan for financial institutions that maintain customer information concerning fewer than five thousand consumers. However, as a best practice, all entities should have a plan- written or otherwise- that addresses response to cyber incidents.

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 company 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 and state regulators in accordance with applicable regulatory 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 (describe below)

RESPOND

19. Has the company 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 company'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

If yes, are any such third parties pre-approved by the company'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 (describe below)

COMMENTS (Optional)

APPENDIX A

IDENTIFY / PROTECT

Controls for Data Backup

This Appendix is a continuation of Question 12. Use the blank column headers to identify these critical services and activities previously identified in Question 4, then check all that apply and provide explanations where needed in the comment box below. For systems data managed by an outside vendor, consider asking the vendor to complete the questions, if necessary. This Appendix may be duplicated if necessary.

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 any authentication process in place below.*	☐	☐	☐	☐
c) At least daily full system (vs incremental) backups are made. *If not, describe any backup process in place 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.*	☐	☐	☐	☐

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 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 company 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 backups here.

a.)

b.)

c.)

d.)

e.)

f.)

g.)

h.)

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 and companies. This resource and others listed below are actionable and can help companies 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 Site: https://www.csbs.org/ransomware-self-assessment-tool

US Secret Service Guidance on Preparing for a Cyber Incident: https://www.secretservice.gov/investigations/cyberincident