Ransomware Self-Assessment Tool

December 2020

Developed by 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

This nonbank Ransomware Self-Assessment Tool (R-SAT) was derived from the R-SAT developed to protect the banking industry. It contains important controls that ALL types of companies should use to assess their efforts to mitigate risks associated with ransomware[1] and to identify opportunities for increasing security. The original R-SAT was developed by the Bankers Electronic Crimes Taskforce (BECTF), State Bank Regulators, and the United States Secret Service. While there are references to resources used by the banking industry, these resources are useful for all types of industries.

Ransomware is a type of malicious software (malware) that encrypts data on a computer, making it difficult or impossible to recover. The attackers usually offer to provide a decryption key after a ransom is paid; however, they might not provide one or it might not work if provided, which could make the company's critical records unavailable. Companies that pay ransoms not only encourage future ransomware attacks but may also risk violating federal regulations[2].

Accurate and timely completion of the assessment, as well as periodic re-assessments, will provide management and the board of directors (as applicable) with an overview of the entity's preparedness towards identifying, protecting, detecting, responding, and recovering from a ransomware attack. This could also assist third parties (such as auditors, security consultants and regulators) that might also review your security practices.

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

Due to the sophistication of this threat, some areas in the tool are mildly technical. You may want to ask your vendors and third-party service providers to complete some questions.

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 *(if applicable)*:	

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

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

IDENTIFY/PROTECT	
1. Have you implemented a comprehensive set of controls designed to mitigate cyber-attacks (e.g. Center for Internet Security's (CIS) Critical Security Controls [3])?	□ YES □ NO
What standard(s) or framework(s) are used to guide cybersecurity control implementation[4]? Check all that apply. *Note: State bank regulators do not endorse any specific standard or framework.*	□ AICPA SOC □ CIS Controls □ COBIT □ FFIEC CAT □ FSSCC Cybersecurity Profile □ ISO □ NIST Cybersecurity Framework □ PCI DSS □ Other (List 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 you use?	□ YES □ NO
3. Is the institution covered by a cyber insurance[5] policy that covers ransomware? If yes, please provide the name of the insurer.	□ YES □ NO

[3] Refer to Center for Internet Security's The 20 CIS Controls & Resources

[4] American Institute of CPAs System and Organization Controls (AICPA SOC), Center for Internet Security's (CIS) Controls, Control Objectives for Information Technologies (COBIT), Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT), Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile, 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 the FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs

IDENTIFY/PROTECT

4. It is important to know the location of the institution's critical data and who manages it. List your primary systems or activities and indicate if they are processed or performed internally or are outsourced to a third party, such as vendors that specialize in Core or that provide network administration (aka Managed Service Providers or MSPs). If a system is not used, please leave the boxes unchecked.

	In-House	Outsourced
Primary Core System	□	□
Network	□	□
Email Service	□	□
Image System	□	□
BSA/AML Systems	□	□
Other Critical Systems (Please List below):		
	□	□
	□	□
	□	□
	□	□

IDENTIFY/PROTECT

5. 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 that they have (such as remote scripting, patching, sharing screens, VPN, etc.)

If yes, are controls implemented to prevent ransomware and threat actors from moving from the third-party's network to the institution's network via these types of access?

□ YES □ NO

If yes, describe the controls.

Have all third-party vendors with remote access provided an independent audit that confirms these controls are in place?

□ YES □ NO

6. Do risk assessments include ransomware as a threat? □ YES □ NO

If yes, are common potential attack vectors (e.g., phishing, watering holes, malicious ads, third-party apps, attached files, etc.) identified?

□ YES □ NO

IDENTIFY/PROTECT

7. Have all ransomware risks and threats identified in risk assessments been appropriately remedied or mitigated to an acceptable risk level?	□ YES □ NO

8. Indicate which of the following are included annually as part of employee security awareness training. (Check all that apply.)

□ Ransomware

□ Social engineering and phishing

□ Incident identification and reporting

□ Phishing email testing to evaluate effectiveness of training

□ None of the above

IDENTIFY/PROTECT

9. Indicate which controls have been implemented for backing up the primary core system and network data. (Check all that apply and provide explanations where needed in the comment box below.) For other critical data, use the form in the Appendix. If any of this data is managed by an outside vendor, consider asking the vendor to complete the questions.

Controls	Primary Core System	Network
a) Procedures are in place to prevent backups from being affected by ransomware. (Please describe on next page.)	□	□
b) Access to backups use authentication methods that differ from the method used to access the network. (If not, please describe on next page.)	□	□
c) At least daily full system (vs incremental) backups are made. (If not, please describe on next page.)	□	□
d) At least two different backup copies are maintained, each stored on different media (disk, cloud, flash drive, etc.) and are stored separately. (Please describe on next page.)	□	□
e) At least one backup is offline, also known as air gapped or immutable. (Please describe method on next page.)	□	□
f) A formal backup testing process is used at least annually to ensure the institution can recover from ransomware using an unaffected backup copy.	□	□

IDENTIFY/PROTECT

Describe controls.

IDENTIFY/PROTECT

10. Indicate which of the following preventative controls have been implemented. (Check all that apply.)

□ Remote Desktop Protocol (RDP) is disabled, 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 an “Allow list” (aka whitelist).

□ Multi-Factor Authentication (MFA) is used (Check all that apply below):

   □ by all users that access any cloud-based service (such as mortgage origination, HR platforms, etc.)

   □ for cloud email services (such as Office 365)

   □ for VPN remote access into the network

   □ with an app that generates a security code (vs a push text/SMS code)

   □ for at least administrative access

□ Administrative access to endpoints, workstations, and network resources is restricted to network support personnel.

□ “Least privileged access” to shared folders and other resources has been adopted.

□ Active Directory provisioning and review (especially for service accounts) is actively managed and reported to management.

□ Unnecessary browser and email client plugins have been disabled.

□ Maintenance and enforcement of network-based URL and DNS filtering has been established.

□ Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) that detect and block ransomware, including exchanging encryption keys, has been established.

□ Domain-based message authentication, reporting, and conformance (DMARC) is in place and set to at least quarantine status.

□ Behavior-based malware prevention tool(s) are in place. (List below.)

□ Network segmentation is used to prevent spread of ransomware and the movement of threat actors across the entire network.

IDENTIFY/PROTECT

11. Is the threat of ransomware specifically included (such as a scenario) as part of the annual test of the incident response plan?	□ YES □ NO
Does executive management participate in testing at least annually?	□ YES □ NO
Does the CEO participate in testing at least annually?	□ YES □ NO

DETECT

12. Indicate which of the following monitoring practices for servers, workstations, networks, endpoints, and backup systems are utilized. (Check all that apply.)

□ Data Loss Prevention Program that provides alerts for (and prevents) large amounts of data from being exfiltrated by the ransomware.

□ Alerts (and blocking) of executable files attempting to connect to the Internet.

□ Active monitoring of network management tools used on workstations, such as Windows Management Instrumentation (WMI) and PowerShell (PsExec).

□ Detection of suspicious file extensions.

□ Detection of large amounts of file renaming.

□ None of the above.

RESPOND

13. 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

RESPOND

14. Indicate which of the following ransomware response procedures are included in the Incident Response Plan. (Check all that apply.)

- □ Contact legal counsel and cyber insurance company (if applicable) so they are immediately notified.
- □ Prepare document for internal staff to use when responding to customer questions.
- □ Establish procedures to ensure forensic information and audit logs are preserved before any restoration is performed.
- □ Determine the scope of the infection by hiring specialized third parties or, if appropriately experienced, by using in-house or MSP resources.
- □ Prevent or isolate the ransomware from spreading to other systems.
- □ Contact federal law enforcement as they periodically obtain decryption keys for some variants of ransomware and they know how to preserve digital evidence.
- □ Determine the cause of the incident.
- □ Mitigate all exploited vulnerabilities.
- □ Restore systems/data (if needed).
- □ Notify incident response stakeholders.
- □ Periodically update contact information for firms that assist with incident response.
- □ Notify all affected employees, customers, and/or vendors as warranted.
- □ Notify stakeholders as appropriate (employees, board, stockholders).
- □ A specific individual(s) is given the authority to shut down a third-party's access to the network.
- □ Contact regulators.
- □ Other ____________________

15. If third parties will be engaged, do contact information and/or pre-arranged service contracts exist so that legal and contract issues do not delay the response?	□ YES □ NO

RECOVER

16. Indicate which of the following are included in return to normal operations procedures. (Check all that apply.)

□ User testing after restoration.

□ After action review to identify lessons learned.

□ Updating the Incident Response Plan with lessons learned.

□ Notifying stakeholders as appropriate (employees, board, stockholders).

□ Other: ______________________________

COMMENTS (Optional)

APPENDIX

IDENTIFY / PROTECT

Controls for Data Backup

Identify other “critical data” not addressed in question 9 and insert the data type in the column headings for the table below. Indicate which controls have been implemented for backups of that data. (Duplicate this appendix if necessary.)

Other “critical data” should be identified in question 4 and may include:

- Online Systems
- Email Services
- Image Systems
- BSA/AML Systems

If any of this data is managed by an outside vendor, consider asking the vendor to complete.

Controls	***Data Type:***	***Data Type:***	***Data Type:***
a) Procedures are in place to prevent backups from being affected by ransomware. (Please describe on next page.)	□	□	□
b) Access to backups use authentication methods that differ from the method used to access the network. (If not, please describe on next page.)	□	□	□
c) At least daily full system (vs incremental) backups are made. (If not, please describe on next page.)	□	□	□
d) At least two different backup copies are maintained, each stored on different media (disk, cloud, flash drive, etc.) and stored separately. (Please describe on next page.)	□	□	□
e) At least one backup is offline, also known as air gapped or immutable. (Please describe on next page.)	□	□	□
f) A formal backup testing process is used at least annually to ensure the institution can recover from ransomware using an unaffected backup copy.	□	□	□

APPENDIX

IDENTIFY / PROTECT

Controls for Data Backup

Comments on Controls