**Ransomware Self-Assessment Tool**

**OCTOBER 2020**

# *Developed by 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 developed this tool. It was developed to help financial institutions assess their efforts to mitigate risks associated with [ransomware](https://www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf)[[1]](#footnote-2) 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.

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 financial institution’s critical records unavailable. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations[[2]](#footnote-3).

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

The Ransomware Self-Assessment Tool is derived from the BECTF *Best Practices for Banks: Reducing the Risk of Ransomware* ([June 2017](https://www.csbs.org/sites/default/files/2017-11/BECTF%202017%20Best%20Practices_Ransomware%20Final.pdf)), which have been updated for today’s environment. Accurate and timely completion of the assessment, as well as periodic re-assessments, will provide executive management and the board of directors with a greater understanding of the financial institution’s ransomware preparedness and areas where improvements can be made. This could also assist other third parties (such as auditors, security consultants and regulators) that might also review your security practices.

Due to the sophistication of this threat, some areas in the review 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**: | | | |
| **IDENTIFY/PROTECT** | | | | |
| 1. Are the Center for Internet Security (CIS) controls**[[3]](#footnote-4)** used to mitigate the most common cyber-attacks? | | YES  NO | | |
| What other standard(s) or framework(s) (if any) are used to guide cybersecurity control implementation**[[4]](#footnote-5)**? | | FFIEC CAT   FSSCC Cybersecurity Profile   NIST (National Institute of Standards and Technology)   ISO   PCI DSS   AICPA SOC   COBIT  Other\_Annual IT General Controls Review, Internal Vulnerability Scans, External Penetration Tests, Social Engineering Campaigns | | |
| 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  IT Risk Assessment performed with ransomware risk mitigated to acceptable levels.  FFIEC CAT completed and meeting maturity levels based on inherent risk or meeting all baseline maturity declarative statements.  Identified items are being remediated or have been approved by the Board.  NO | | |
| 1. Is the institution covered by a cyber insurance**[[5]](#footnote-6)** policy that covers ransomware? If yes, please provide the name of the insurer.  |  | | --- | | Enter Name of Insurer here | | | YES  NO | | |

|  |
| --- |
| **IDENTIFY/PROTECT** |
| 1. It is important to know the location of the institution’s critical data and who manages it. Indicate if the following systems or activities 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).  |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  | **In-House** |  | **Outsourced** | | Core Processing |  |  |  | | Network Administration |  |  |  | | Email Services |  |  |  | | Image Files (Checks, Loans, etc.) |  |  |  | | Trust |  |  |  | | Mortgage Loans |  |  |  | | Investments (Bonds, Stocks, etc.) |  |  |  | | Other Critical Data (Please List below): |  |  |  | | Retail Online Banking |  |  |  | | Business Online Banking / ACH Portal for Business Customers |  |  |  | | Spam Filtering Solution |  |  |  | | Refer back to R.A. or at a minimum, think through the critical systems. |  |  |  | |

|  |  |
| --- | --- |
| 1. 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.)   |  | | --- | | Remote access for patch management, network support, etc. Silent remote access allowed. |   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.   |  | | --- | | Speak with your network support vendor regarding their controls. Some examples could include what type of antivirus the network support vendor is using, whether 2FA is used for remote access to the bank’s network, etc. |   Have all third-party vendors with remote access provided an independent audit that confirms these controls are in place?  YES  NO Note: if No, look at SGC website and request that enhanced due diligence be completed (SGC -> Services -> Templates). | |
| 1. Do risk assessments include ransomware as a threat? If they don’t, then add ransomware either as it’s own information / infrastructure asset or add it as a risk to each critical asset. | YES  NO |
| If yes, are common potential attack vectors (e.g., phishing, watering holes, malicious ads, third-party apps, attached files, etc.) identified? Somewhere in the risk assessment, phishing and other related items should be covered.  YES  NO | |
| 1. Have all ransomware risks and threats identified in risk assessments been appropriately remedied or mitigated to an acceptable risk level? | YES  NO |
| 1. Indicate which of the following are included annually as part of employee security awareness training programs. (Check all that apply.)   Ransomware – Remember, ransomware is a type of malware. Make sure to at least define ransomware for personnel – what it is and what it does, but there should be a focus on malicious websites and downloading malicious attachments.  Social engineering and phishing – Cover phishing, hovering over links, what to look out for to identify suspicious emails, phone attacks, in-person attacks (e.g., pest control), USB drop attacks (even when USB is blocked, there are ways around this), etc.  Incident identification and reporting – What types of things to look out for (e.g., unusually slow computer, random files deleting, etc.) and who to report this to.  Testing to ensure effective training – Simulated phishing and other social engineering campaigns. We suggest letting employees know this will be happening and that the campaigns can use attacks that may seem unfair – hackers don’t care about fairness.  None of the above | |
| 1. Indicate which controls have been implemented for backing up Core Processing and Network Administration data. (Check all that apply and provide explanations where needed in the comment box below.) For other critical data, such as Trust services, Mortgage Loans, Securities - Investments, and others, use the form in the [Appendix](#_APPENDIX). If any of this data is managed by an outside vendor, consider asking the vendor to complete the questions.  | **Controls** | **Core Processing** | **Network Admin** | | --- | --- | --- | | 1. Procedures are in place to prevent backups from being affected by ransomware. (Please describe below.) |  |  | | 1. Access to backups use authentication methods that differ from the network method of authentication. (If not, please describe below.) |  |  | | 1. At least daily full system (vs incremental) backups are made. (If not, please describe below.) |  |  | | 1. At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.) and they are stored separately. (Please describe practice below.) |  |  | | 1. At least one backup is offline, also known as air gapped or immutable. (Please describe method below.) |  |  | | 1. A regular backup testing process is used at least annually that ensures the institution can recover from ransomware using an unaffected backup. |  |  | | |
| Some examples might include (just suggestions):   * Network (and core system backups if applicable) are performed daily to another location with a weekly backup disconnected from the network. * Backups are segmented with access to backups through port rules and time restricted (logical segregation of backups). * Antivirus protection is on all end points. * Even better, **next generation antivirus** is used on all endpoints, or at a minimum, on the backup server. NGAV tools focus on Indicators of Attack as opposed to Indicators of Compromise. * Backups are replicated offsite; offsite backups are considered immutable. * Network (and core system backups if applicable) use non-domain credentials or different credentials that those of domain admins. * Macro files (.docm, xlsm, etc.) are blocked by spam filtering. * Users do not have local admin capabilities. * Application whitelisting is in place. * Workstations, laptops, servers, etc. are patched frequently (e.g., weekly) – 3rd party and Microsoft. * SIEM or LEM implemented on all critical servers. * Spam filtering is in place for all incoming email. * Firewalls with IDS / IPS implemented and monitored … * Document your primary controls that are in place. | |
| 1. 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 whitelisted. Ask your network support vendor.  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.) – MFA should be implemented wherever offered and wherever possible.  for cloud email services (such as Office 365) – every time for web based email and for mobile device, on some frequency (e.g., every 14 days).  for VPN remote access into the network – utilizing hardware or soft token authentication is ideal (e.g., duo, FortiToken, etc.).  with an app that generates a security code (vs a push text/SMS code)  for at least administrative access  Eliminated administrative access to endpoints, workstations, and network resources for all but network support personnel.  Adopted “least privileged access” concept for granting users access to shared folders and other resources.  An established process for provisioning and reviewing Active Directory access (especially for service accounts) is actively managed and reported to management.  Disabled all unnecessary browser or email client plugins.  Maintenance and enforcement of network-based URL and DNS filtering. Check with your managed firewall provider.  Use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) that detect and block ransomware activity including exchanging encryption keys.  Implementation of domain-based message authentication, reporting, and conformance (DMARC) policy and set to at least quarantine status.  Use of behavior-based malware prevention tool(s).   |  | | --- | | Some examples can include Sophos Intercept X EDR, CrowdStrike, Carbon Black Cloud, Cylance, etc. |   Network segmentation to prevent spread of ransomware and the movement of threat actors across the entire network. At a minimum, consider segmenting backups. | |
| 1. Is the threat of ransomware specifically included (such as a scenario) as part of the annual test of the incident response plan?   Some example scenarios might include.   * John Doe downloaded a file containing malware that encrypted his hard drive only. * John Doe downloaded a Word document which encrypted his hard drive, as well as all of his mapped shared drives. * John Doe clicked on a link to a malicious website which ultimately led to a fileless attack using Power Shell to encrypt the contents of his hard drive and all share drives. * A malicious actor was able to establish positive control (communication with a command and control server) and has begun to move laterally on the network to identify critical systems. | 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** |
| --- |
| 1. 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. Exfiltration (leakware / doxware) – typically we see this with our larger banks closer to the $1 billion asset size.  Alerts (and blocking) of executable files attempting to connect to the Internet.  Active monitoring of network management tools used on workstations, such as WMI (Windows Management Instrumentation), PsExec, and other power shell scripts. NGAV solutions – EVERY bank, should at least evaluate some of these and implement accordingly.  Detection of suspicious file extensions. Firewall monitoring, spam filtering, policies.  Detection of large amounts of file renaming. SIEM, LEM  None of the above. |

| **RESPOND** | |
| --- | --- |
| 1. Does the Incident Response Plan identify a person (internal or third-party) with the expertise to manage/coordinate all aspects of a ransomware response? This will typically be the bank’s ISO or IT individual, but could be anyone – the incident response plan just needs to identify this individual. | YES  NO |
| 1. Indicate which of the following ransomware response procedures are included in the Incident Response Plan. (Check all that apply.) If these aren’t in the current plan, make a section called Ransomware or Malware (Ransomware Included) and, if accurate, document each of these as part of the plan. If not planning on doing any of the below, consider doing so.   ☐ 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. This could be a formal document, or it could be simply informing front-line staff of how to respond to customer questions.  ☐ Establish procedures to ensure forensic information and audit logs are preserved before any restoration is performed. Contact SIEM or LEM vendor. If no SIEM or LEM, involve network support vendor.  ☐ 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. (e.g., unplug ethernet cable from impacted devices, shut off ports, if using NGAV, quarantine device(s)).  ☐ Contact federal law enforcement as they periodically obtain decryption keys for some variants of ransomware and they know how to preserve digital evidence. Contact FBI.  ☐ 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 incident 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. We suggest contacting both state and federal regulatory authorities.  ☐ Other­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| 1. 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** |
| --- |
| 1. Indicate which of the following are included in return to normal operations procedures. (Check all that apply.) Similar to above, if the below will be completed, document this within your incident response place under ransomware, or even malware recovery.   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)** |
| Enter additional comments here. |

## 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:

* Trust services
* Mortgage Loans
* Securities - Investments
* Email Services
* Image files (checks, loans, etc.)

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

| **Controls** | ***Insert Data Type Here*** | ***Insert Data Type Here*** | ***Insert Data Type Here*** |
| --- | --- | --- | --- |
| 1. Procedures are in place to prevent backups from being affected by ransomware. (Please describe on next page.) |  |  |  |
| 1. Access to backups use authentication methods that differ from the network method of authentication. (If not, please describe on next page.) |  |  |  |
| 1. At least daily full system (vs incremental) backups are made. (If not, please describe on next page.) |  |  |  |
| 1. At least two different backup copies are maintained, each is stored on different media (disk, cloud, flash drive, etc.) and they are stored separately. (Please describe on next page.) |  |  |  |
| 1. At least one backup is offline, also known as air gapped or immutable. (Please describe on next page.) |  |  |  |
| 1. A regular backup testing process is used at least annually that ensures the institution can recover from ransomware using an unaffected backup. |  |  |  |

**APPENDIX**

**IDENTIFY / PROTECT**

**Controls for Data Backup**

|  |
| --- |
| **Comments on Controls:**  **Provide commentary here regarding controls implemented for additional critical data that isn’t covered in question 9, or if covered in question 9, indicate as such.** |

1. Refer to Federal Financial Institutions Examination Council (FFIEC) [Joint Statement Cyber Attacks Involving Extortion](https://www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf) [↑](#footnote-ref-2)
2. Refer to FinCEN Advisory [Ransomware and the Use of the Financial System to Facilitate Ransom Payments](https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a006) and OFAC [Ransomware Advisory](https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001) [↑](#footnote-ref-3)
3. Refer to Center for Internet Security’s [The 20 CIS Controls & Resources](https://www.cisecurity.org/controls/cis-controls-list/)   
    [↑](#footnote-ref-4)
4. Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT), Financial Services Sector Coordinating Council (FSSCC), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Payment Card Industry Data Security Standard (PCI DSS), American Institute of CPAs System and Organization Controls (AICPA SOC), Control Objectives for Information Technologies (COBIT) [↑](#footnote-ref-5)
5. Refer to the  [FFIEC Joint Statement - Cyber Insurance and Its Potential Role in Risk Management Programs](https://www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20Cyber%20Insurance%20FINAL.pdf) [↑](#footnote-ref-6)