fnbo

Ransomware Reference Document

INFOSEC

protecting your assets

Information Security
It's everyone's business.
Our customers expect it.

Contents

Introduction

This document aims to help our customers plan for, improve resilience to, or recover from a ransomware attack.

The document is designed to organize critical processes during the lifecycle of an incident and provide guiding principles. It incorporates different stakeholder involvements, allowing teams to respond appropriately and limit the risk and exposure.

This document is intended to increase and enhance existing company policies when a suspected ransomware occurrence is recognized. It is not intended to supplant, annul, replace, or eliminate existing playbook, runbook, or strategy.

What is ransomware?

Ransomware is a type of malware (malicious software) designed to subvert security controls for the purpose of denying an organization access to their own data or systems it infects. The organization must pay a fee to the threat actor to recover the data. Ransomware attacks are constantly on the rise and represent a top technology risk worldwide. Organizations with mature cybersecurity practices are more resilient to these types of attacks.

A ransomware attack is a type of extortion by a threat actor which takes advantage of weakness in an organization's cybersecurity controls. Data is often transferred externally (exfiltrated), and some strains will seek to destroy or encrypt internal backups to render the backups useless. The threat actor will then demand payment in exchange for the decryption keys, and an agreement to not release the stolen data to the public.

The payment demand is usually made in crypto currency so that it will not be traceable.

Threat actors are generally anonymous and deceptive. Any agreements or deals convey a significant risk and do not guarantee recovery. Complying can result in only partial recovery, forced secondary payments, and still present operational impacts, costs, and losses the organization hoped to avoid through payment. The average downtime of a ransomware attack is 23 days. The average cost of a ransomware breach is now $4.6m.

Making payments to criminal enterprises, or nation state threat actors can also be a violation of OFAC or other US Laws and regulations. Consult with your legal department or legal representative and have a formal policy to guide your decisions.

Recommendations for ransomware resilience

Ransomware attacks can be devastating if the proper measures are not taken to mitigate the risk of an attack. Below are the five primary function of ransomware resilience: preparation, prevention, detection, mitigation, and recovery. This ransomware recovery plan can be depicted as follows:

Prepare

"Every Technology Risk Executive must work with the Business to translate the 1's and 0's into $'s and ¢, to make the right resource investments to protect their brand and their clients."

- Brian Fricke, Chief Information Security Officer, City National Bank of Florida

Technology asset management

A clear understanding of critical business systems, and information assets will enable informed decisions when developing any type of protection and recovery plan. A complete inventory of all Information Assets (Key data, key systems of record, support systems, etc.) is the first step to enabling the protection of those assets.

Business continuity planning

Clear documentation of critical business processes, including your vendor provided services, will provide greater resilience in the event of a ransomware disruption to the systems that underpin those business processes. A complete inventory of all Critical Business Processes and the systems they rely on is required for success. Documentation of workarounds, alternate processes, and alternate vendors you can leverage during an outage will help you minimize the overall impact to your customers while the affected system by ransomware is restored. The average downtime due to a ransomware attack is 23 days. The business continuity plan should include notification requirements and contact information for your vendors and financial institutions so they can assist your company to continue critical processes and minimize impact.

Risk assessment

Gathering certain attributes about your Business Applications (e.g. they contain sensitive data, execute transactions, are accessible from the internet, hosted in house/vendor provided etc.) will help you prioritize the protection (implementation of security controls) for those assets based on their risk/ impact to the organization if they were affected by ransomware. The risk assessment will allow you to focus your capital investments where you need it most to minimize impact to your customers or financial impact to your revenue during an attack.

Incident response retainer

Pre-establishing an Incident Response Retainer with a qualified security firm will help expedite your response to a successful cyber-attack. This contract for services allows you to bring in experts who can help respond to the breach, augmenting your internal staff during the crisis. If your company buys cyber insurance, check with your cyber insurance provider to see if the company you selected is pre-approved by your cyber insurance provider. This will help you minimize your out-of-pocket costs during a crisis. Fee based models may allow for the "activation" of the retainer for penetration testing, resilience exercises such as tabletops, etc., annually if it has not been used in a real response that calendar year.

Cyber insurance

One way to transfer some of the financial impact/risk due to a security incident is to carry a separate cyber policy by your insurer. These policies typically have coverage specifically for ransomware and what liabilities and coverage are present. It is imperative that your insurance provider be involved as soon as you declare an incident of ransomware to assist in decision making, funding, and reporting requirements.

Executive involvement

Ransomware's goal is to receive money. If ransomware is detected within your company, it is helpful to create a matrix of options for payment. This does not mean you will pay, but it provides leadership with the ability to make an informed decision with the pros and cons of paying. The matrix should address your risk appetite, at what threshold your company is willing to absorb a disruption versus paying the ransom. Note, facilitating a payment to a sanctioned country may violate OFAC rules.

Roles and responsibilities

Cybersecurity should be fundamentally important for each organization. A group of devoted people who understand the risks and have the specialized abilities to fabricate a solid framework need to assist with guaranteeing that the network is safeguarded. This group should be completely engaged with all parts of IT; they need to have dynamic power and impact across all recovery plan and preparation decisions. To ensure the cybersecurity team is adequately prepared to deal with threats, they should be staffed, well-funded, and trained. The organization should ensure that their cybersecurity team's skill set will improve and advance through continuous training as ransomware attackers convey new strategies.

You can define key role assignments to detection, mitigation, and recovery tasks. These roles may become involved during an incident. These individuals may appoint delegates for their roles depending upon the circumstances of a specific incident. One of the key roles to define is your Cybersecurity Incident Response Team (CSIRT) and Incident Response (IR) Team. These teams will help your company manage through the crisis and will be involved during test exercises to ensure your plans are effective.

Regular backups with integrity testing

Ransomware attacks rely on access to an organization's data and information and will frequently include the deletion of data. Therefore, a robust backup/recovery plan is crucial to restoring the business to a well-known state. Consider these recommendations for your backup program:

- Ensure that all backups are encrypted when data is in transit and at rest.
- Regularly audit your backup program to ensure what data is being stored can be restored.
- Perform frequent tests by restoring data and system configuration from your backups.
- The 3/2/1 rule is defined as keeping three copies of your data for critical assets across two media types (local and cloud) and one backup stored in an offsite location. Ensure that at least one copy is immutable. Immutable backups cannot be modified or rendered useless by ransomware.

By maintaining offline or immutable backups, updating them, and often verifying their usability, your organization can minimize the impact of a successful ransomware attack and prevent severe disruptions.

Tabletop exercises

Plans are great for threat modeling, training, and coordination among stakeholders, but in a crisis, it can often go out the window if not well tested. The only way to know whether a Response Plan will work is to test it. It is impossible to think of everything when developing a plan. Testing will uncover issues and help an organization work to resolve them. Test plans require updates as changes in the environment and personnel occur. Establishing a process to regularly test and improve the response plan is essential.

Continuous validation

It is essential to proactively validate and continue to look for opportunities to advance. Working with an independent third party with cybersecurity expertise will help any organization double-check the strategy and identify cracks.

Prevent

"The best defense against ransomware is preventing it—and it's more important than ever for companies and employees to work to prevent cyber incidents through training and good user behavior."

Paul Tucker, Chief Information Security Officer, BOK Financial

Awareness and training

Every organization should have a well-established program to train and educate all personnel on the safe use of email, and of the systems they use for their day-to-day work. Phishing is the primary method of initial attack that result in breaches. Testing your staff awareness on identifying malicious emails and having a mechanism in place for them to report these to your security team is key to preventing an attack. This is your first line-of-defense against attacks.

Least privilege

Enforcing the "least privilege" principle is an effective defense against the rapid spread of ransomware once it has infected company systems. Basically, the principle states that company personnel have the absolute bare minimum of access rights necessary to carry out their job. If a subject does not need an access right, the subject should not have that right.

Cyber hygiene (Patch and vulnerability management)

Technology is constantly evolving as bugs are discovered, and improvements are made. Security updates or patches are designed to mitigate vulnerabilities that have been identified in your organization's operating environment. Waiting to make these updates increases the probability of an attacker capitalizing on these weaknesses. Organizations should work on updating systems soon after the release of a security update. Prioritization is also necessary, as certain assets may have a greater risk, and organizations should look to utilize a centralized management system to simplify the execution and oversight of security updates.

Multifactor authentication

Passwords are utilized for safeguarding systems and their data, yet complex malicious actors can still find ways around passwords in some cases. Organizations should execute multifactor authentication by utilizing passwords with access tokens to limit this risk. This further progression will make it difficult for culprits to access the network. Multifactor authentication can be laid out by utilizing regenerative access tokens that lapse quickly. Associations can use different gadgets as an extra guardrail and use an application or SMS messaging to produce the access token.

Endpoint detection and response (EDR)

Ransomware attackers will search for any point of weakness in an organization's network safety and immediately penetrate. Organizations have various access points to their frameworks, and it may be an unimaginable task to safeguard each entry point continuously. To guarantee that dangers are distinguished and wiped out, organizations should use other technology to find suspicious movements and unapproved activities. Checking devices and logging activity of any kind will assist with recognizing ransomware aggressors. Furthermore, associations need to have controls and automated actions to limit the harm when a ransomware attacker effectively gets to the framework, and cycles should be created to respond. Once distinguished, automation ought to confine the passage point from the remainder of the framework, access should be eliminated, all passwords should be reset, and all resources should be supported. Organizations should be ready for the worst- case scenario and have plans and abilities to respond to any threat.

Encryption

Data and resources have worth to the organization, and attackers will hope to use anything as an influence to extort an organization. In the case of effective penetration, everything is at risk. As an extra layer of security and to postpone and frustrate the attackers, everything that can be encrypted should be. Encryption changes all data into an ambiguous format that cannot be re-established without the encryption key. All significant data at rest and in transit should be encrypted, and encryption keys should be secured in a separate location with additional protective controls. This should especially be applied to any sensitive consumer information collected and protected under the Consumer Financial Protection Act (CFPA). Encryption can assist an organization with safeguarding valid details by making them unusable to an attack.

Network segmentation

Ransomware attacks look to both steal data and disrupt operations. Segregating different business functions onto separate networks will help contain the damage, minimize the cost, and maintain operations in the event of a successful attack. The more barriers between different processes and sets of valuable information, the more difficult it will be for an attack to critically disrupt the business.

Detect

"Ransomware can put your company out of business forever. Early detection allows companies to quickly react and contain the impact a ransomware attack has on customers, revenue, reputation, and ultimately the ability for the company to survive."

Rudy Ramirez, Chief Information Security Officer, Citizens Business Bank

Ransomware detection may originate from alerting, threat hunting, user notification, and third parties. The goal of the detection phase is to confirm a ransomware-related event has occurred and assess the scope, risk, and impact of the incident. Activate the Incident Response (IR) process when there is potential for adverse business impact and preserve crucial evidence for the investigation of the incident.

Responding to alerts

It is critical for an organization to review and respond to security alerts. Often, security alerts will notify security and information technology teams of a potential issue such as a ransomware attack. As the teams review alerts, ensure there is correlation of security alerts against other systems as a ransomware attack can trigger different alerts in various systems. Alert correlation can help you minimize the time to confirm the attack and begin mitigation.

Swift assessment

Perform a swift assessment of the impact once the confirmation of a ransomware attack is received. This will enable your company to isolate affected systems and reduce the ability for the ransomware attack to spread into other areas within your company. During your assessment, include your backup system to ensure it is operational. Also assess the ability for your company to perform a restore from your backup system.

Notification

Upon confirmation of the attack, engage your legal department or legal representative. In addition, under legal guidance, notify your insurance carrier and security vendors. Notifying your insurance carrier and security vendors under guidance from your legal department will start the process to receive technical assistance for the mitigation of the attack. You may also want to consider seeking guidance from your legal department on notifying other partners that are directly connected to your company. This notification may allow your partner to act to minimize or prevent the ransomware attack from spreading into their computer system.

Incident response team activation

Consider activating your response team that will help your company during the event. The response team will ensure that all steps required are taken. During a crisis, you need a team that has participated in test exercises to carry out the steps necessary to successfully recover from a ransomware attack. There are technical and administrative tasks that need to be completed including notification requirements of the event based on your contractual agreements with vendors and customers or regulatory notification requirements for regulated institutions and public companies.

Mitigate

"Mitigation is where the investments made in preparation, the efforts expended in prevention, and the tools deployed in detection coalesce. Practitioners and executives should be focused on mitigatory responses that isolate and minimize damage, lessen the impact of the event, and generate strategies to prevent a future reoccurrence."

Endre Jarraux Walls, EVP, Chief Information Security Officer, CUBI Security Group

During the Mitigation phase, the company will develop a containment strategy to isolate the impacted resources (network segments, users, facility, and region) to stop the propagation of ransomware. There are multiple containment levels, such as host-based, network-based, and user/ identity-based containment. As necessary, containment activities may be undertaken in parallel with the identification-related activities.

Level	Mitigation considerations
Network	· Security system rule changes · Block specific traffic/packet patterns via intrusion detection system (IDS) or next-generation firewall (NGFW) · Block via a network device (routers, etc.) · Implement Domain Name System (DNS) sinkholes for known Command and Control (C2) traffic
Host	· Disable the network port of the host · Leverage endpoint detection and response (EDR) software or network security groups to restrict host communications · Block malicious file execution · Disable or lock-down infected endpoints
User/identity	· Disable account · Change password · Invalidate or expire user sessions · · Disable applications authenticating with user credentials, tokens, or certificates
Physical	· Disable employee card access keys · Change access key PIN (if applicable) · Secure the perimeter of the facility · If applicable, contact law enforcement
Other methods	· Email Isolation (inbound email)

Resource isolation and removal considerations

Ransomware-related incidents rapidly evolve, and information is progressively revealed during IR efforts. CSIRT personnel will often need to make containment decisions based on limited information quickly. Performing isolation or removal actions may have an adverse business impact in and of themselves. Still, the CSIRT has the authority to make such decisions exigently when currently available incident information indicates that failure to take such actions immediately has a high likelihood of causing more significant adverse business impact(s).

	Containment considerations
1	Develop the containment strategy while using best efforts to assess business impact and resource isolation/removal considerations: · Identify potential physical safety impact on employees · Determine which systems are known to be infected · Identify systems within network reach that could be soon impacted and the methods by which they could be impacted · Identify how the spread of ransomware to such systems could be prevented · Identify the business/application owners who need to be contacted · Determine who may need to be notified
2	Finalize the containment strategy, including the determination of the scope of systems/applications that will be included in the containment actions: · Identify impacted account(s) that may need to be disabled · Inoculate systems based on ransomware behavior (e.g., if the malware exists based on the presence of specific files or mutexes, these conditions could be created on noninfected systems to "inoculate" these systems from infection) · Addition of security controls · Harden other at-risk systems · Increase security monitoring, including scanning the environment for known indicators of compromise
3	Implement the containment strategy.
4	To mitigate other adverse business impact, the IRTeam may take actions to rapidly prevent or contain the spread of ransomware or other threat actor operations in the corporate environment. CSIRT may do this by isolating or removing any of the following from the company's network: · Specific user(s) · Specific device(s) · Specific application(s) or service(s) · Specific environment(s) · the Company facility(s) · Geographic region(s)
5	The IR team may need to obtain approval from Senior Leadership to take drastic containment steps that may have an adverse business impact. Such decisions are necessary to prevent an even more significant negative impact on operations.
6	Establish a timeline of the incident (what has occurred so far?). Identify the earliest indication of attacker activity and keep in mind when considering what backups to leverage (if applicable).
7	Assume that account credentials that were used to authenticate with infected systems are compromised. Reset these passwords and disable and re-issue accounts (the latter may be prudent for certain domain administrator accounts, depending on incident circumstances).

Recover

The goals of the recovery phase are to restore operations, provide ongoing support and communications to impacted employees and customers, begin decryption and data recovery/ restoration while minimizing the risk of re-infection, perform credential resets based on trust, and remediate the cause of the incident rapidly and safely.

Data recovery considerations

Prioritize recovery of systems based on business impact, leveraging business continuity planning (BCP) tier assignments and Disaster Recovery (DR) classifications.

Most ransomware threat actors target backups, including local Windows volume shadow copies and online backup solutions. Verify whether such backups are available and leverage them when and where they are.

	Data recovery considerations
1	· Prioritize recovery of systems and services based on business impact leveraging the Business Impact Analysis (BIA).
2	· Ensure that the recovery platform and tools are safe and that no malicious programs have been installed before or during the recovery process by the threat actor. · Restore from backup(s) to a sandboxed environment, where feasible · Perform integrity checks on golden images to ensure the attacker has not altered them · Ensure the attacker has not planted or left behind malicious software in backups · Scan recovered data for viruses and malware · Search for known Indicators Of Compromise (IOCs) in the recovered data · Validate the integrity of recovered data
3	· Check for local volume shadow copies on Windows hosts (and validate whether the ransomware deletes these).
4	· Deploy and configure a temporary environment for reimaging and testing systems before enterprise deployment. · If using a temporary environment is not practical, recover data in place but consider segmentation between the known clean and "dirty" environments to prevent re-infection.
5	· Rebuild or reimage systems infected by malware (including but not limited to the ransomware) and interacted with by the attacker (e.g., remote access, reverse shells, command-and-control beacons/ agents, etc.). Reimaging should be performed off a "golden" image or backup that meets the Recovery Time Objective (RTO)/Recovery Point Objective (RPO) for the system.
6	· Where data recovery is not possible or when challenges occur, work with business units and file owners to understand the impact (e.g., unable to restore from backup, backup contains outdated or partially corrupted data, etc.).
7	· As necessary, remove any isolation/segmentation controls when containing the incident.
8	· Provide regular status updates to the senior leadership liaison.

Password reset strategy checklist

After ransomware has been detected, contained, and remediated, it is essential to reset affected account passwords if potential credential compromise has occurred. While managing the incident, consider the following before passwords are reset:

	Password reset strategy considerations
1	• Before passwords can be reset, mitigating controls should be enforced. Some controls include – Implement or enable MFA for remote access (e.g., VPN, OWA, etc.) – Reset active VPN connections – Remove any old/stale AD/AAD or VPN accounts – Disable any unauthorized remote access software (e.g., Go2myPC, TeamViewer, VNC, etc.) – Confirm there are no internet-accessible systems with unintentionally exposed services (e.g., RDP, SSH, etc.) – Reset all affected account(s) passwords
2	• To reset Windows Active Directory passwords, consider the following: – Rebuild all affected domain controllers – Reset all accounts, not just affected accounts » This includes administrator and service accounts » During the post-incident phase, reset all accounts for a second time » This should happen once there is reasonable confidence the attacker is no longer in the environment – Reset the Kerberos Ticket Granting Ticket (KRBTGT) account twice per Microsoft's recommendations

Conclusion

We hope this guidance document helps our customers organize critical processes during the lifecycle of an incident and provides guiding principles.