CITIZENS BUSINESS BANK

A Financial Services Company



Ransomware Reference Document

Contents

Introduction

This document aims to help Citizens Business Bank 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 the 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 the Office of Foreign Assets Control's (OFAC) regulations and other U.S. laws and regulations. Consult with your legal department 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 functions of ransomware resilience: preparation, prevention, detection, mitigation, and recovery. This ransomware recovery plan can be depicted as follows:

Prepare

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 system affected 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 with continuing 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 on your customers or financial impact on 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 legal agreement for services (often at no cost up front) 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 annual "activation" of the retainer (for penetration testing, resilience exercises such as tabletops, etc.) 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 as a result of 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 ultimate 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.

If ransomware is impacting your customer and they facilitate a payment to a sanctioned country, this would 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 create a solid framework needed 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.

Using Appendix A, you can define key role assignments for detection, mitigation, and recovery tasks. These roles may become more active during a security incident. These individuals may appoint delegates for their roles depending upon the circumstances of a specific incident. One of the key roles to define 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, and
- 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.

Prepare continued

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

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 results 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 Privilege of Least principle is an effective defense against the rapid spread of ransomware once it has infected company systems. Basically, the principle states that company personnel should 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 access 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.

Prevent continued

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 encoded 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

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. In addition, under the guidance of your legal department, notify your insurance carrier and security vendors. Notifying your insurance carrier and security vendors under the guidance of 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 and 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.

Detection checklist

Additional information and steps can be found in the Detection checklist located in Appendix A.

Mitigate

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 needed, containment activities may be undertaken in parallel with the identification-related activities.

Mitigate continued

Level	Activity	Typically involved	Authorized by
Physical	• Disable employee card access keys. • Change access key PIN (if applicable). • Secure the perimeter of the facility. • If applicable, contact law enforcement.	• Physical security team	• CSIRT
Other methods	• Email Isolation (inbound email)	• IR team	• CSIRT

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 checklist

	Containment checklist	Responsible
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 soon be 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, and • Determine who may need to be notified.	• Senior leadership • CSIRT director • IR team
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, and • Increase security monitoring, including scanning the environment for known indicators of compromise.	• Senior leadership • CSIRT director • IR team
3	Implement the containment strategy.	• CSIRT director • IR team

Mitigate continued

	Containment checklist	Responsible
4	To mitigate other adverse business impact, the IR Team may take actions to quickly 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(ies), and/or • Geographic region(s).	• CSIRT director • IR team
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.	• Senior leadership
6	Establish a timeline for 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).	• CSIRT
7	Assume that account credentials 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).	• CSIRT • IT team

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 checklist

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.

Recover continued

	Data recovery checklist	Responsible
1	• Prioritize recovery of systems and services based on business impact leveraging the Business Impact Analysis (BIA).	• CSIRT director • IR team • DR team
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.	• CSIRT director • IR team
3	• Check for local volume shadow copies on Windows hosts(and validate whether the ransomware deletes these).	• CSIRT director • IR team
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.	• CSIRT director • IR team
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.	• CSIRT • IR team
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.).	• CSIRT director • IR team
7	• As necessary, remove any isolation/segmentation controls when containing the incident.	• CSIRT director • IR team
8	• Provide regular status updates to the senior leadership liaison.	• CSIRT director

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 checklist	Responsible
1	• Before passwords can be reset, mitigating controls should be enforced. Some controls include: — Implementing or enabling MFA for remote access (e.g., VPN, OWA, etc.), — Resetting active VPN connections, — Removing any old/stale AD/AAD or VPN accounts, — Disabling any unauthorized remote access software (e.g., Go2myPC, TeamViewer, VNC, etc.), — Confirming there are no internet-accessible systems with unintentionally exposed services (e.g., RDP, SSH, etc.), and — Resetting all affected account(s) passwords.	• CSIRT director • IR team
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 that the attacker is no longer in the environment; and — Reset the Kerberos Ticket Granting Ticket (KRBTGT) account twice per Microsoft's recommendations.	• CSIRT director • IR team • Communications • Legal

Conclusion

Citizens Business Bank hopes this guidance document helps you organize critical processes during the lifecycle of an incident and provides guiding principles.

Appendix A – Additional checklists

Roles and responsibilities chart

Name	Title	Ransomware playbook role(s)
CSIRT director		
IR team		
IR team		
Enterprise resiliency		
Legal		
Communications		
Senior leadership		
Senior leadership liaison		
Executive stakeholder		

External parties		
	Law enforcement	
	Digital forensics and IR (DFIR)	
	Crypto broker	
	Cyber Insurance	
	Outside counsel	

Communications considerations

The organization (or its designated negotiator/crypto broker) should follow the communication workflow outlined below as the leading practices and follow up with the attacker every 1–3 days with the next step. This can be done even if the company does not intend to pay the ransom, as an optional stalling strategy.

If, during threat actor communications, the attacker's name, email address, or writing style changes, perform decryption validation steps again to verify the attacker's ability to decrypt the data.

	Communications checklist	Responsible
1	• If applicable, create a believable fictitious persona to communicate with the threat actor throughout the negotiation process. • Create a throwaway email account for this persona. • If possible, consider also creating a LinkedIn profile for the fictitious persona. — This can be done before any incident so that it only must be activated/deactivated as needed. — This step helps keep communications with the attacker, limits their ability to infect other company systems, and keep some degree of anonymity	• CSIRT • Crypto broker
2	During negotiation, stall the process by "validating" with internal groups the negotiation terms.	• Crypto broker • Legal/outside counsel
3	During negotiation, if it is not already known, ask the threat actor to confirm/validate whether data was exfiltrated as part of the attack.	• CSIRT • Legal/outside counsel • Crypto broker
4	If possible, ask the threat actor how they were able to enter and move laterally through the environment.	• CSIRT • Legal/outside counsel • Crypto broker
5	If data has been exfiltrated and the company is paying the ransom, ask for a secure deletion log of the data from the threat actor and confirmation that no other copies of the exfiltrated data are in their possession	• CSIRT • Legal/outside counsel • Crypto broker

Decryption strategy checklist

If decryption keys are obtained, the Incident Recovery team must balance the need to restore operations and prevent reinfection. Guidelines include:

	Decryption strategy checklist	Responsible
1	• Trained incident responders should handle decryption software and reverse engineer any software supplied by the attacker to determine whether it contains additional exploits or other security concerns. • Where applicable and possible, the decryption key(s) should be extracted from any software provided by the attacker and used with software vetted by the company (and a trusted third party) for the decryption of files.	• CSIRT director • IR team • Third-party DFIR consultant
2	• If decryption software has been obtained from the threat actor, a segregated environment may be set up for decryption efforts, and files may be scanned with security software (e.g., antivirus) before their re-introduction to the "clean" environment. • Test decryption software in a sandboxed and controlled environment before using it widely. • The attacker may have planted malware or other files alongside your company's data during their activity in the environment, which the ransomware may have also encrypted.	• CSIRT director • IR team • Third-party DFIR consultant • Crypto broker
3	• Data should be decrypted in order of priority, where possible. • For decrypting at scale, once a decryption key has been scanned and validated, consider creating copies and distributing system resources so that multiple systems can be decrypted simultaneously.	• CSIRT director • IR team
4	• Decryption software modifies data in place. For critical data, consider making a copy of the encrypted files and first attempting to decrypt the copied data (this enables recovery should the decryption software fail and further corrupt the data).	• CSIRT director • IR team
5	• Sometimes files may not decrypt successfully; this is a concern for databases, which may not be fully encrypted by ransomware (and therefore also not successfully decrypted). Making copies of encrypted data before decrypting helps prevent corruption. Incident responders and data recovery specialists might be able to recover data from specific file formats if they were not successfully encrypted in their entirety (e.g., databases).	• CSIRT director • IR team

Decryption validation checklist

Decryption validation involves sending a sample of encrypted documents to the threat actor for confirmation that the attacker (a) is responsive, and (b) can decrypt the files. This can be used when contemplating paying the ransom or as an optional stalling strategy to divert the threat actor while further progress is made in IR and recovery efforts.

	Decryption validation checklist	Responsible
1	• Compile a sample set of files that were encrypted by ransomware. • If the ransomware encrypted the files with multiple keys, identify files from various stages of keys to help ensure the attacker can decrypt all encrypted data. • Identify files from numerous systems and environments.	• CSIRT • DFIR consultant • Business owner(s) • Legal/outside counsel
2	• Validate the sample set of documents compiled in the first step • Confirm that the sample files were successfully encrypted in their entirety and are of a file type that can be easily validated using low-risk commercial software. • Determine that sample files contain only low sensitivity information.	• CSIRT • DFIR consultant • Legal/outside counsel
3	• Send the sample set of files to the attacker • Facilitate communications through the Crypto broker and follow general communications guidance	• CSIRT • DFIR consultant • Legal/outside counsel • Crypto broker
4	• Validate the attacker's response via their ability to decrypt selected files. • Any files or attachments received from the attacker should be treated as malicious and handled by technical incident responders. • Files received from the attacker should be opened in a sandboxed environment and scanned for viruses or other security exploits. • Confirm that the file(s) received are the exact file(s) sent to the attacker. • Assess whether the files were successfully decrypted in their entirety (i.e., can they be opened in their standard associated software). • Coordinate with the file owner or business unit to determine whether the decrypted file contents are accurate and expected (i.e., verify the attacker did not send alternative files back that were not sent as examples for decryption, or the attacker did not send false data).	• CSIRT • DFIR consultant • Legal/outside counsel • Crypto broker

If the attacker cannot decrypt any file(s), it may mean that the attacker cannot decrypt some or all encrypted data. If this occurs, you may wish to re-engage the decryption validation process with another set of files (either as a stalling strategy or to assess further the attacker's ability to decrypt all relevant data should payment be made). Consider sending sample files from priority keys to confirm that critical data can be decrypted in situations with multiple keys. Do not reveal to the attacker which keys are more important than others, as this may harm negotiations.

General recovery checklist

In addition to the above steps, consider the following items:

	General recovery checklist	Responsible
1	• Submit a cyber insurance claim, if applicable.	• Insurance coordinator • Legal
2	• Develop a strategy to repair reputation, if needed.	• Senior leadership • Communications • Legal
3	• Prepare any reporting materials for the Senior Leadership Liaison or the Company Senior Leadership.	• CSIRT director • Senior leadership • Legal
4	• Review communication plan and update process to address any gaps or insufficiencies.	• CSIRT director • Senior leadership • IR team • Communications • Legal

Detection checklist

When conducting an initial assessment of the ransomware event, the following checklist can assist in assessing the nature of the incident:

	Detection checklist	Responsible
1	Gather information and validate that a ransomware event has occurred. Initial questions and actions include: • Has an initial timeline been established? • Has an alert related to the detection of ransomware been triggered? • Any suspicion on the initial point of entry? • How is the malware spreading? • Has a ransom note been identified? If so, take a screenshot of this. — What ransomware family/strain has been used? — What is the file extension of the ransom note? • What systems, accounts, and data are impacted (e.g., servers, user machines, etc.)? • How sensitive is the data stored, processed, or transmitted by the affected systems? • What operating systems are impacted? • Do the systems or data targeted affect a single person, team, customer(s), department, or the whole of the company? • How widespread is the incident? Estimate the breadth of the incident (e.g., visible on a certain number of systems or contained to a specific VLAN, etc.) — How many systems are on the network? — How many are encrypted? • How many systems have a similar configuration and could also be vulnerable and affected?	• CSIRT director • IR team

	Detection checklist	Responsible
	• If possible, leverage incident tracking through a ticketing system or Security Orchestration Automation and Response (SOAR) technology to centralize collected information from this step, utilizing the following records to gather data where applicable to the incident: — Account of Interest, — Host of Interest, — Vulnerability of Interest, — Behavior of Interest, and — File of Interest.	
2	Conduct an initial assessment of the event to determine the scope and impact: • Criticality of data/systems involved (as per High-Value Asset (HVA) list), • Number of systems/endpoints affected, • The probability of the event increasing in severity, • The physical location of data/systems involved, and • Effect on customers, employees, and the company leadership (i.e., disclosure of sensitive information, disruption to business processes, etc.) In the absence of a criticality rating, Cybersecurity Incident Response Team (CSIRT) will initiate an initial incident classification based on the evidence collected thus far, assigning classification levels P1 through P4.	• CSIRT director • IR team
3	Conduct assessment of disaster recovery/backups below. • Assess the availability and integrity of backups and snapshots. • Are backups/snapshots encrypted or removed? • If any backups are available, immediately preserve (e.g., isolate backup server(s) and consider shutting down if actively encrypting to prevent further data encryption – but note the risk of corruption by doing so). • Do any systems affected have redundancy arrangements?	• CSIRT • IR team
4	• Consider if the Incident Response (IR) process should be activated. The IR process may be started for an incident that could adversely impact the business. • CISO/IR Team assess if this event could adversely impact the business if not managed effectively. • CISO calls for IR Team review. • If the IR process is activated, assemble the Incident Team (IR Team).	• CSIRT director • IR team
5	Engage Risk team to notify cyber insurance provider if the incident threshold may approach the predetermined percentage of retention. Consider having Legal coordinate the engagement of all third parties with the insurance coordinator going forward to help ensure successful response activities.	• Insurance coordinator • Legal • IR team
5a	• Consider the engagement of Outside Counsel to establish and maintain privilege.	• Legal
5b	• Consider the engagement of third-party forensic investigators.	• CSIRT • Legal/outside counsel • CISO • Insurance coordinator • Third-party DFIR consultant

	Detection checklist	Responsible
6	Discuss and identify SEC, regulatory, and external auditor reporting, timelines, and requirements.	• Legal • Outside counsel • Senior leadership
7	Start investigation consistent with IR plan including consideration of the following below. • Determine root cause. • Identify ransomware family and any other identified malware. • Was the detection the result of a live or on-demand scan? • Have you identified/classified antivirus vendors? • Have legitimate system users (s) been asked whether they know why the ransomware is present? • How does ransomware propagate? • Was the ransomware launched/pushed from a remote host? • Credentials used by an attacker.	• Legal/outside counsel • CSIRT director
8	If applicable, determine the "categories" of data that may have been impacted for data privacy/notification considerations: • Data access: Interactive access, accessed directory, and files; and • Data exfiltration: Evidence of data archive and transfer	• CSIRT • Legal/outside counsel • Third-party DFIR consultant
9	Assess whether the incident is being used to divert attention away from a breach or another attack. Avoid "tunnel vision" — do not neglect routine, ongoing cybersecurity monitoring across the environment.	• CSIRT • CSIRT director
10	Inform company personnel that external communications are only to be done according to company policy and may only be informed by authorized individuals. • Unauthorized individuals must be instructed not to speak to the press or post on any social media.	• Legal • Communications
11	Submit a cyber insurance claim, if possible.	• Insurance coordinator • Legal


CITIZENS
BUSINESS BANK
A Financial Services Company