NATIONAL CYBERSECURITY CENTER

Ransomware Incident Response Initial Steps

LIMIT THE SPREAD ***Identify the impacted systems and turn off network access.***	• If several systems/computers or subnetworks appear impacted, take the network offline at the switch level. It may not be possible to disconnect individual systems during an incident. • If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection. • BEWARE: DON'T tip off the bad actors that you know that you have been compromised. Bad actors often monitor your organization's activity and communications to determine if their compromise has been detected. Isolate systems in a coordinated manner and use things like phone calls or in-person conversations (if possible) to address the compromise. If you use communication that is on the system, the bad actors may be able to track your moves and stay ahead of you to preserve their access – or even deploy ransomware widely before you take the network offline.
POWER DOWN ***BUT ONLY in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.***	Note: This step will prevent you from maintaining ransomware infection artifacts and potential evidence that can be used to catch the bad actors. Powering down should only be carried out if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.
PRIORITIZE YOUR SYSTEMS ***Identify critically impacted systems for restoration and recovery.***	• Identify and prioritize critical systems for recovery and restoration, and confirm what type of data is on those systems. NOTE: This process is much easier to do if you have already worked through your critical assets, including systems necessary for health and life safety, personally identifiable information, revenue generation, or other critical services. • Take note of the systems and devices that do not appear to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.
DOCUMENT WHAT HAPPENED ***Work with your team to develop and document an initial outline of what occurred.***	• Work with the first responders to the incident on your team to identify when the first indicator of compromise (IOC) was noticed, how it presented itself (files blocked, ransom note, etc.), and the initial steps taken to control the damage. • Next identify what steps were taken to preserve the critical systems and ensure their continued operation. • Document who was contacted and when within your organization (as well as any outside help you may have sought) to ensure that all necessary individuals were notified.
GET SUPPORT ***Engage your internal teams and stakeholders, as well as outside entities that can help***	• Use the contact sheet below to connect with the most important people within your organization (e.g. departmental and elected leaders) and external entities that can help. External entities include your cyber insurance provider (if you have one), local or state jurisdictions with which you have a mutual aid agreement in place, CISA, MS-ISAC's CERT team, among others. NOTE: Don't be afraid to share! By reaching out to these internal and external groups ASAP, you have a MUCH better chance of getting the issue resolved, and for less time and money.

CONTACT

INFO@CYBER-CENTER.ORG

Office: (719) 255-5225

State and Local Response Contacts

Contact	24x7 Contact Information	Roles and Responsibilities
IT/IT Security Team		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Checklist for Local Governments Utilizing IT Vendor

Question	Information	Notes
Who is the contact person within your organization that will notify the IT vendor?		
Who is the primary contact of the IT vendor?		
Have you discussed the IR policies and procedures with your IT vendor?		*If no, stop filling this out and contact your IT vendor immediately.*
What is written into your service contract regarding IR?		*Identify where a hard copy is kept, as well as a link to an electronic file (ideally password-protected)*
How often does your vendor perform backups on your data?		
How much access does the vendor have to your organization's data?		
Does your IT vendor have an internal IR plan for any or all of their customers?		*If no, STOP filling this out and work with them to develop one for your organization. If they don't want to, look for another IT vendor.*
Has your IT vendor performed any IR activities with other organizations before?		
Does your vendor have any relationships with other vendors to perform IR?		*If yes, identify who, and what their process is for contacting that additional vendor. Also determine if there are any additional costs associated with contacting that vendor.*

CONTACT

INFO@CYBER-CENTER.ORG

Office: (719) 255-5225