New River

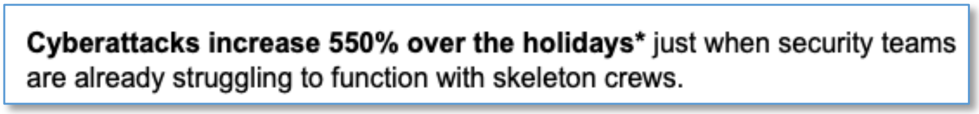
Community and Technical College

Ransomware Attack:

Incident Response Playbook

Amid the chaos, there is also opportunity.

- Sun Tzu



Cyberattacks increase 550% over the holidays* just when security teams are already struggling to function with skeleton crews.

Version:	1.0 (December 6, 2023)
Authors:	David J. Ayersman and Gary P. Davis
Approval Authority:	Vice President and Chief Information Officer

Executive Summary

This playbook is a guide that should be followed for responding to ransomware incidents. It establishes procedures that should be deployed, exercised, and governed as part of the overall cybersecurity and incident response plans and procedures.

Post-incident response efforts should routinely include updates to this information.

Playbook Applicability – Ransomware Attack

A ransomware incident involves a piece of malicious software which has been successfully executed on a system. The code could be targeted and bespoke (customized to a particular customer or user) or generic. Ransomware is a specific subset of malware that is designed to block access to a computer system or data on a computer system, usually until a sum of money is paid for a decryption key. Industry best practice and recommendations from law enforcement and compliance agencies is to *never* pay the ransom, as it does not guarantee a decryption key will be received and it only encourages bad actors to continue their illegal efforts.

Ransomware generally has two types:

1) **Locker ransomware**—locks the computer or device, and
2) **Crypto ransomware**—prevents access to files or data, usually through encryption.

There are predictable steps and measures that an organization should follow in response to a ransomware attack. This Playbook details these steps in two (*customized for New River*) formats: (1) a short summary that can be followed quickly during initial triage and (2) a lengthier and more detailed series of enumerated steps to guide efforts after initial containment efforts have been successful (see Appendix A).

Initial 3-Step Triage

1. Verify and Notify
2. Investigate, Respond, and Report
3. Analyze and Preserve

Complete 4-Step CISA Recommended Response

CISA (2023) recommends responding to ransomware by using the following four steps:

1. Detection and Analysis (*Verify*)
2. Reporting and Notification
3. Containment and Eradication (includes *Preservation of Evidence*)
4. Recovery and Post Incident Activity

Initial 3-Step Triage

1 Verify and Notify (*All Users*)

Users play a critical role in promptly by (1) identifying ransomware attacks, (2) notifying IT support, and (3) limiting the scope of the damages by powering down infected devices.

a) Has a Ransomware message appeared on the screen?
   YES → use cell phone to take a picture and then shutdown (or remove the device from the network) and proceed to NOTIFY.
   NO → If in the process of encrypting and the message has not yet appeared, immediately shutdown or remove from the network (and NOTIFY).
   Unsure?→If you are unsure of what to do and believe you have been compromised, shutdown the device or remove from the network (and NOTIFY).

b) NOTIFY the CIO, CISO, or CTO—using an immediate method of SMS, Zoom, or phone call (regardless of the day or time) and the **Contact Information** at the end of this document.

2 Investigate, Respond, and Report (*CIO, CISO, and CTO*)

Microsoft Defender for Endpoint is the EDR (Endpoint Detection and Response) solution used by New River.

c) Did EDR detect Ransomware? (Y/N)
   - (a) YES → Investigate ransomware in Windows Defender Security Center (auto investigation should begin)
   - (b) NO → Notify Microsoft that EDR failed to detect ransomware. Determine why it was not detected and investigate further to gather more details.
   - (c) If further investigation reveals additional IoCs (Indicators of Compromise), document them and use them to mitigate if possible.

d) Shared File Locations
   - i) Check for encrypted files.
   - ii) Disable backup scripts until ransomware is contained.

e) Damage Assessment
   - i) Internal
     - (1) How many endpoints were affected?
     - (2) How many servers were affected?
     - (3) Were backups affected?
     - (4) Was shared folder location affected?
   - ii) External
     - (1) Have there been any threats/comments made on social media? (Facebook, Twitter, Instagram, etc.)
     - (2) Notify 3rd party vendors and agencies (see **Contact Information**).
       - (a) Alpha Technologies
       - (b) WVNET

(c) HEPC (legal counsel, CISA, DHS, and FBI)

iii) Criticality of Impacted Devices

(1) How sensitive is the data stored, processed, or transmitted by the affected systems (use Data Classification system defined in Information Security Procedure—*Public, Sensitive, Highly Sensitive*).

(2) How critical are the services provided by the affected systems?

(3) Do the targeted systems or data affect a single person, team, business unit, or whole organization?

(4) What other systems are on the same subnet as the affected systems? (Network Segmentation Diagram is helpful)

(5) Which systems are affected and how sensitive is the data that is stored?

(a) How much data is affected?

(6) Are there data availability, integrity, or confidentiality issues?

(a) Where does the data reside and how is it accessed? (endpoints, network drives, cloud storage)

iv) VPN

(1) Disable VPN (*with support from Alpha and WVNET*).

(2) If EDR has been disabled, work with vendors to terminate VPN sessions and prevent further sessions (this should occur within first 5-10 minutes or endpoint will likely be lost).

3 Analyze and Prepare for Recovery (*CIO, CISO, and CTO*)

f) Identify the type and name of ransomware if possible.

g) Is there any evidence provided to indicate a specialized or targeted function?

h) Does the ransomware target specific data/system(s)?

i) Is there any evidence of data being exfiltrated?

j) How were systems infected?

i) What attack vectors were used?

ii) If ransomware propagated and affected multiple systems, was it done so automatically or did it require user interaction?

k) Network

i) Identify users, devices, and services the ransomware is communicating with.

ii) What does threat intelligence say about the addresses?

iii) Will this stop services or just slow them down?

iv) Is Packet Capture Analysis available?

v) What is the payload analysis?

2. Recovery/Mitigation

a) Backups?

i) Full, incremental, or differential?

ii) Shared folders and drives?

iii) Cloud services (OneDrive, Dropbox, iCloud, Google Cloud, etc.)

(1) EDR should notify us of the threat, and it will provide options to recover OneDrive files (Files Restore) to the state prior to the attack.

b) Search Enterprise for ransomware Indicators of Compromise (IOC's)

c) Implement additional countermeasures as a lesson learned.

Complete 4-Step CISA Recommended Response

After implementing the previous three triage steps, a pause can be taken to understand the attack more fully, this allows for the most effective response. These four steps recommended by CISA can ensure an overall effective response.

1. Detection and Analysis

Refer to the best practices and references below to help manage the risk posed by ransomware and support New River's coordinated and efficient response to a ransomware incident. Apply these procedures to the greatest extent possible based on availability of organizational resources.

1. **Determine which systems were impacted, and immediately isolate them.**
    - If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
    - Prioritize isolating critical systems that are essential to daily operations.
    - If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
    - For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigation.
    - After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access or deploy ransomware widely prior to networks being taken offline.
2. **Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.**
    - **Note:** This step will prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. **It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network** using other means.
3. **Triage impacted systems for restoration and recovery.**
    - Identify and prioritize critical systems for restoration on a clean network and confirm the nature of data housed on impacted systems.
        - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.

    - Keep track of systems and devices that are not perceived 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.

4. **Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) and logs.**

- Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.
    - Look for evidence of precursor “dropper” malware, such as Bumblebee, Dridex, Emotet, QakBot, or Anchor. A ransomware event may be evidence of a previous, unresolved network compromise.
        - Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network to further extort the victim and pressure them into paying.
        - Malicious actors often drop ransomware variants to obscure post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromises.

5. **Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**
6. **Initiate threat hunting activities.**

For **enterprise** environments, check for:

a) Newly created AD accounts or accounts with escalated privileges and recent activity related to privileged accounts such as Domain Admins.
b) Anomalous VPN device logins or other suspicious logins.
c) Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations. Look for anomalous usage of built-in Windows tools such as bcdedit.exe, fsutil.exe (deletejournal), vssadmin.exe, wbadmin.exe, and wmic.exe (shadowcopy or shadowstorage). Misuse of these tools is a common ransomware technique to inhibit system recovery.
d) Signs of the presence of Cobalt Strike beacon/client. Cobalt Strike is a commercial penetration testing software suite. Malicious actors often name Cobalt Strike Windows processes with the same names as legitimate Windows processes to obfuscate their presence and complicate investigations.
e) Signs of any unexpected usage of remote monitoring and management (RMM) software (including portable executables that are not installed). RMM software is commonly used by malicious actors to maintain persistence.
f) Any unexpected PowerShell execution or use of PsTools suite.
g) Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz or NTDSutil.exe).
h) Signs of unexpected endpoint-to-endpoint (including servers) communications.
i) Potential signs of data being exfiltrated from the network. Common tools for data exfiltration include Rclone , Rsync, various web-based file storage services (also used by threat actors to implant malware/tools on the affected network), and FTP/SFTP.
j) Newly created services, unexpected scheduled tasks, unexpected software installed, etc.

For **cloud** environments:

a) Enable tools to detect and prevent modifications to IAM, network security, and data protection resources.
b) Use automation to detect common issues (e.g., disabling features, introduction of new firewall rules) and take automated actions as soon as they occur. For example, if a new firewall rule is created that allows open traffic (0.0.0.0/0), an automated action can be taken to disable or delete this rule and send notifications to the user that created it as well as the security team for awareness. This will help avoid alert fatigue and allow security personnel to focus on critical issues.

2. Reporting and Notification

Note: Refer to the **Contact Information** section at the end of this guide for details on how to report and notify about ransomware incidents.

- Follow notification requirements as outlined in your cyber incident response and communications plan to **engage internal and external teams and stakeholders** with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.
    - Share the information you have at your disposal to receive timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders (CISA, 2023b).
    - Report the incident to—and consider requesting assistance from—CISA, your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or your local U.S. Secret Service field office.
    - As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.
- If the incident resulted in a data breach, **follow notification requirements as outlined in your cyber incident response and communications plans**. An example statement to standardize communication might be:

"Since the College first became aware of this incident an investigation was started and we have been methodically working to determine the nature and scope of the incident. Our focus right now is getting services back online for students and employees. More information will be released by the President at a later date."

3. Containment and Eradication

If no initial mitigation actions appear possible:

- **Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers)**. Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.

  - Preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).
- **Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available**, as security researchers may have discovered encryption flaws for some ransomware variants and released decryption or other types of tools.

To continue steps to contain and mitigate the incident:

- **Research trusted guidance** (e.g., published by sources such as the U.S. Government, MS-ISAC, or a reputable security vendor) for the ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.
  - Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known associated registry values and files.
- **Identify the systems and accounts involved in the initial breach.** This can include email accounts.
- Based on the breach or compromise details determined above, **contain associated systems that may be used for further or continued unauthorized access.** Breaches often involve mass credential exfiltration. Securing networks and other information sources from continued credential-based unauthorized access may include:
  - Disable VPN, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.
- If server-side data is being encrypted by an infected workstation, **follow server-side data encryption quick identification steps.**
  - Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.
  - Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.
  - Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.
  - Review the Windows Security log, SMB event logs, and related logs that may identify significant authentication or access events.
  - Run packet capture software, such as Wireshark, on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., smb2.filename contains cryptxxx).
- **Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.**
  - Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
  - Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).

  - Identification may involve deployment of EDR solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.
- **Rebuild systems based on prioritization of critical services** (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible. Use infrastructure as code templates to rebuild cloud resources.
- **Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility** once the environment has been fully cleaned and rebuilt, including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms. This can include applying patches, upgrading software, and taking other security precautions not previously taken. Update customer-managed encryption keys as needed.
- **The designated IT or IT security authority declares the ransomware incident over** based on established criteria, which may include taking the steps above or seeking outside assistance (BRIM provides breach response team to assist).

4. Recovery and Post Incident Activity

When defensive measures fail, an organization must resort to recovery. After that, plans must be improved based on the lessons learned.

- **Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.**
  - Take care not to re-infect clean systems during recovery. For example, if a new VLAN has been created for recovery purposes, ensure only clean systems are added.
- **Document lessons learned from the incident and associated response activities** to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.
- **Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC** to benefit others within the community.

Approved by:

CIO (Chief Information Officer)

David J. Ayersman, Vice President and Chief Information Officer

__________________________________ 11/23/2023

Signature Date

Contact Information

(New River Employees)

CIO (Chief Information Officer)

David J. Ayersman, Vice President and Chief Information Officer
Office: 304-256-0281
Cell: 304-384-0992
Email: dayersman@newriver.edu

CISO (Chief Information Security Officer)

Gary P. Davis, Director of Information Security
Office: 304-
Cell: 304-
Email: gdavis@newriver.edu

CTO (Chief Technology Officer)

Jason L. Garris, Director of Technology Development
Office: 304-
Cell: 304-
Email: jgarris@newriver.edu

(Vendors, Compliance Agencies, and Law Enforcement)

Alpha Technologies

Open ticket in Alpha Helpdesk with high severity level. CIO will send SMS to Alpha CEO.

Alpha Helpdesk URL:	http://help.alpha-tech.us/support
Alpha Helpdesk Phone:	304-201-7485

WVNET

Open ticket in OZ with high severity level.

WVNET Helpdesk URL:	https://oz5.wvnet.edu/ozwvnet/
WVNET Helpdesk Phone:	304-293-5192

HEPC (need designated contact info)

They notify BRIM, legal counsel, and federal agencies on behalf of New River.

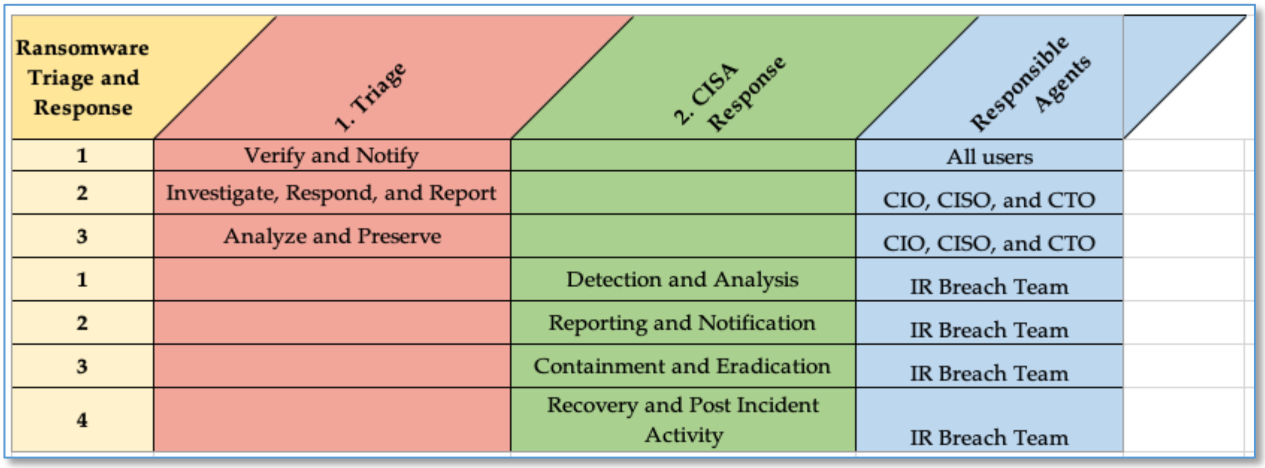
HEPC Helpdesk URL:	https://
HEPC Helpdesk Phone:	304-

CISA (FBI, DHS, and Secret Service)

HEPC reports to CISA, and they share with FBI, DHS, and others.

https://www.cisa.gov/stopransomware/report-ransomware

APPENDIX A. RANSOMWARE RESPONSE STEPS AND RESPONSIBLE AGENTS



Ransomware Triage and Response	1. Triage	2. CISA Response	Responsible Agents
1	Verify and Notify		All users
2	Investigate, Respond, and Report		CIO, CISO, and CTO
3	Analyze and Preserve		CIO, CISO, and CTO
1		Detection and Analysis	IR Breach Team
2		Reporting and Notification	IR Breach Team
3		Containment and Eradication	IR Breach Team
4		Recovery and Post Incident Activity	IR Breach Team

REFERENCES

CISA. (2023, May). *I've been hit by ransomware!* Cybersecurity and Infrastructure Security Agency CISA. Retrieved November 18, 2023, from https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

CISA. (2023b, March). *Cross-sector cybersecurity performance goals*. CISA CPG. Retrieved November 27, 2023, from https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf