BREACH CHECKLIST

For use with tech team responding to breach
Source: CISA Stop Ransomware

Detection and Analysis

- ☐ **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.
  - ☐ 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. Note: This will prevent you 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.
  - ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means 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—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

- ☐ **Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.**

- ☐ **Triage impacted systems for restoration and recovery.**
  - ☐ Identify and prioritize critical systems for restoration, 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.

- ☐ **Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**

- [ ] **Using the contact information below, engage your 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 the most 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.

- [ ] **Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, 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.**
  - [ ] Take care to 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 regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.**

- [ ] **Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular 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 any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:**
  - [ ] Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

- [ ] **Additional suggested actions—server-side data encryption quick-identification steps:**
  - [ ] In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:
    - [ ] 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 any related logs that may identify significant authentication or access events.
    - [ ] Run 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 an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) 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. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex or Emotet.
    - [ ] 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 in an attempt to further extort the victim and pressure them into paying.
    - [ ] Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.

- [ ] **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 endpoint detection and response 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 a prioritization of critical services (e.g., health and safety or revenue generating services) using pre-configured standard images, if possible.**

- [ ] **Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms), issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software and taking other security precautions not previously taken.**

- [ ] **Declare ransomware incident over. This is the responsibility of the designated IT or IT security authority and based on established criteria, which may include taking the steps above or seeking outside assistance.**

- [ ] **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 Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.

- [ ] **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/ISAO for further sharing and to benefit others within the community.**