Ransomware Attack Response Checklist

STEP 1: Disconnect Everything

- [ ] Unplug computer from network.
- [ ] Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC.

STEP 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

- [ ] Mapped or shared drives
- [ ] Mapped or shared folders from other computers
- [ ] Network storage devices of any kind
- [ ] External Hard Drives
- [ ] USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- [ ] Cloud-based storage: DropBox, Google Drive, OneDrive etc.

STEP 3: Determine if data or credentials have been stolen

- [ ] Check logs and DLP software for signs of data leaks.
- [ ] Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files.
- [ ] Look for malware, tools, and scripts which could have been used to look for and copy data.
- [ ] Of course, one of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen.

STEP 4: Determine Ransomware Strain

- [ ] What strain/type of ransomware? For example: Ryuk, Dharma, SamSam, etc.

STEP 5: Determine Response

- [ ] Now that you know the scope of the damage as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

Response 1: If Data or Credentials are Stolen

- [ ] Determine if ransom should be paid to prevent data or credentials from being released by hackers.
- [ ] If ransom is to be paid, you can skip steps #1 and #3 of Response 2 from recovery.

Response 2: If Ransom Is Not Paid and You Need to Restore Your Files From Backup

- [ ] Locate your backups
  - [ ] Ensure all files you need are there.
  - [ ] Verify integrity of backups (i.e. media not reading or corrupted files).
  - [ ] Check for Shadow Copies if possible (may not be an option on newer ransomware).
  - [ ] Check for any previous versions of files that may be stored on cloud storage e.g. DropBox, Google Drive, OneDrive.
- [ ] Remove the ransomware from your infected system.
- [ ] Restore your files from backups.
- [ ] Determine infection vector & handle.

Response 3: Try to Decrypt

- [ ] Determine strain and version of the ransomware if possible
- [ ] Locate a decryptor, there may not be one for newer strains. If successful, continue steps...
- [ ] Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
- [ ] Decrypt files

  Determine the infection vector & handle

Response 4: Do Nothing (Lose Files)

- [ ] Remove the ransomware
- [ ] Backup your encrypted files for possible future decryption (optional)

Response 5: Negotiate and/or Pay the Ransom

- [ ] If possible, you may attempt to negotiate a lower ransom and/or longer payment period.
- [ ] Determine acceptable payment methods for the strain of ransomware:

  Bitcoin, Cash Card etc.
- [ ] Obtain payment, likely Bitcoin:
  - [ ] Locate an exchange you wish to purchase a Bitcoin through (time is of the essence).
  - [ ] Set up account/wallet and purchase the Bitcoin.
- [ ] Re-connect your encrypted computer to the internet.
- [ ] Install the TOR browser (optional).
- [ ] Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been set up for this specific ransom case.
- [ ] Pay the ransom: Transfer the Bitcoin to the ransom wallet.
- [ ] Ensure all devices that have encrypted files are connected to your computer.
- [ ] File decryption should begin within 24 hours, but often within just a few hours.
- [ ] Determine infection vector and handle.

STEP 6: Protecting Yourself in the Future

- [ ] Implement Ransomware Prevention Checklist to prevent future attacks.