RANSOMWARE ATTACK RESPONSE CHECKLIST

1. Disconnect everything

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

2. Determine scope of infection – check the following for signs of encryption

- [ ] Shared or unshared drives or folders
- [ ] Network storage or any kind
- [ ] External hard drives
- [ ] USB storage devices with valuable files
- [ ] Cloud-based storage: Dropbox, Google Drive, Microsoft Onedrive/Skydrive etc.

3. Determine if data or credentials have been stolen

- [ ] Look for a sign from the involved attackers announcing that your data and/or credentials have been stolen.
- [ ] Check logs and DLP software for signs of data leaks.
- [ ] Look for unexpected large archival files (zip, arc or else) 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.

4. Determine Ransomware Variant

- [ ] Determine what ransomware you have been hit with (for example: Ryuk, Dharma, SamSam, etc.)

5. Report to authorities

- [ ] Contact your local cybercrime cell or police station to report your attack

6. Determine your options

A – Pay the ransom

- [ ] Carefully calculate your risk with all stakeholders (legal counsel, law enforcement, cyber insurance carrier, security expert).
- [ ] Decide whether you should pay the ransom or not.
- [ ] Even if you decide to pay up, don't forget to clean-up afterwards.

B – Try to remove the malware

- [ ] Check nomoreransom.org and other internet sources for helpful decryption keys
- [ ] Try to unlock your data without having to pay the ransom

C – Wipe the system & reinstall from scratch

- [ ] Completely wipe all your storage devices and start afresh, installing everything from the bottom up
- [ ] Restore your data by selecting backups that were made prior to the date of the initial ransomware infection
- [ ] Don't rely on System Restores! Since malicious software is typically buried within all kinds of places on a system, it will not be able to root out all parts of the malware.

7. Protecting yourself in the future

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

Keen to learn more?

If you're unsure of where to begin, consider the advice of our Security experts. When you partner with SoftwareONE, you'll know exactly where your risks are and how to protect your assets. Having said this we invite you to have a look at our additional

Ransomware Survival Guide

How can we help you?
Get in touch to find out more about our Managed Security Services!

SoftwareONE AG
Riedenmatt 4
CH-6370 Stans

T. +41 844 44 55 44
E. info@softwareone.com
https://www.softwareone.com/en/solutions/managed-security