

10-Step Ransomware Recovery Plan

If you are dealing with a ransomware incident you may be working under extreme pressure. Ransomware may still be encrypting files, attackers may have issued ultimatums, and your organization will be desperate to get up and running again. **Ask for help, prioritize your actions, communicate clearly, and take care of each other.** We recommend you take the following actions, in order:

1. Contain the attack.

Isolate infected systems or networks to limit the impact of the attack. Your priority should be containing the attack but if you can do so while also preserving evidence by leaving affected systems turned on, do so.

2. Establish the scope of the attack.

Understand what systems and what kind of data are affected, and prioritize critical systems for recovery.

3. Communicate with stakeholders.

Stakeholders may include senior management, PR, your legal team, cyber-insurance providers, security vendors and law enforcement.

4. Seek assistance.

Consider seeking expert assistance from local and national law enforcement, vendors or other third parties familiar with ransomware recovery.

5. Preserve evidence.

With the help of law enforcement and third parties, try to preserve evidence from the attack if you can.

6. Identify the ransomware being used.

This will help you discover if a decryptor is available, and it will inform the specifics of containment and clean up.

7. Contain the breach.

Try to identify systems and accounts used in the initial breach, and any precursor malware or persistence mechanisms left by the attackers.

8. Rebuild systems.

Use known good system images and backups to restore critical systems. Take care to segregate clean systems from affected systems.

9. Reset, patch, upgrade.

Reset passwords, patch and upgrade software, and instigate any additional security checks necessary to prevent a recurrence of the attack.

10. Document lessons learned.

Ransomware is constantly evolving. Use what you have learned from this attack to better prepare for the next one.