4 PHASES OF A RANSOMWARE INCIDENT RESPONSE PLAN

Responding to a detected ransomware attack should be as simple as following your response plan. But that means you need a plan and team in place to make it happen. With the right preparations, a good incident response plan will get you back to normal operations as quickly and painlessly as possible.

Using a four-phased approach, you can ensure your organization is ready for the next ransomware attack.

1 Initial Discovery & Preliminary Steps

Notify the response team

Enable key groups and partners to begin planning for work

Legal

Communications

Cyber Insurance

Questions to ask:

Who knows about the incident, and *what* do they know?

Has anyone had *contact* with the threat actor?

2 Containment and Initial Investigation

Now is the time to make sure the attack can't spread. Don't be pressured to get systems back up and running as quickly as possible.

Remind leadership that immediate containment is the focus

Deploy or use EDR to gain visibility and contain infected endpoint

CONDUCT A THOROUGH INVESTIGATION

1. **SCOPE** the impact of the ransomware
2. **TALLY** how many systems were encrypted
3. **GATHER** options for recovery and restoration

3 Forensic Analysis and Response

Most emergency work should be done by this phase.

Phase length
Days to weeks – or even longer

In-depth investigation and management of fallout

Important questions to answer:

Have we engaged all external parties properly?

Has our data been exposed? If yes, who needs to be notified of potential exposure and consequences of the breach?

4 Recovery

Does the ransom need to be paid?

YES

- Threat actor provides decryption key
- You prioritize data to decrypt
- Start decryption

NO

FINAL STEP: Finish identifying the root cause of the incident and build a list of recommendations and remediations to implement to prevent future incidents.

Cadre can help you build plans for these situations and test your organization's capabilities with custom tabletop exercises. Going through these motions will help you think critically about your policies and procedures – and identify any gaps that you need to address. Together, this will help lower your risk and improve your incident response planning.

GET STARTED

625 Eden Park Drive
Suite 525
Cincinnati, OH 45202

888.TO.CADRE
WWW.CADRE.NET