

# THE FIRST 72 HOURS OF RESPONSE AFTER A RANSOMWARE ATTACK?

01

0 to 1 HOUR

## CONTAIN THE ATTACK

- Isolate affected systems
- Disable compromised accounts
- Stop lateral movement

02

1 to 6 HOURS

## ASSESS IMPACT

- Identify ransomware variant
- Evaluate affected assets
- Verify backups
- Preserve evidence

03

6 to 24 HOURS

## COORDINATE RESPONSE

- Activate Incident Response
- Secure privileged accounts
- Notify leadership & legal
- Contact cyber insurance

04

24 to 48 HOURS

## RECOVER OPERATIONS

- Restore from clean backups
- Validate system integrity
- Reset credentials
- Resume critical services

05

48 to 72 HOURS

## STRENGTHEN SECURITY

- Find the root cause
- Patch vulnerabilities
- Document lessons learned
- Meet reporting obligations

### KEY TAKEAWAY

The first 72 hours determine how quickly your business recovers.  
**Preparation is your strongest defense.**

