

# The First 60 Minutes of a Ransomware Attack

*A Playbook for Executive Response*






---

*A practical executive guide to minimizing operational  
disruption, financial loss, and regulatory exposure.*



# Ransomware is no longer an IT issue. It is a **business disruption event.**

Modern ransomware attacks typically include:

-  System encryption
-  Data theft
-  Operational shutdown
-  Extortion deadlines
-  Regulatory exposure



**Organizations without a structured response plan often lose valuable time during the first hours of an incident.**

# Why Organizations Struggle During Ransomware Incidents

## Common Challenges:

- ↔ Unclear incident leadership
- 📄 Lack of a coordinated response plan
- 🕒 Delayed decision making
- 💬 Uncertainty around insurance and legal obligations
- 🔄 Unverified backup recovery processes



**The first few hours of a ransomware attack often determine the scale of operational disruption.**

# Who Must Be Involved Immediately

Key stakeholders typically include:

**Executive Leadership**

CEO

CIO/CISO

CTO

**Legal Counsel**

Guides regulatory notifications and protects legal privilege.

**Cybersecurity Incident Response Team**

IT Security

Infrastructure Teams

Legal and Compliance

Communications

Operations Leadership

# Executive Response Timeline

## The First 60 Minutes

What leadership teams must determine immediately after a ransomware event is detected.

**0-5 Minutes**



### Detection and Initial Escalation

- Suspicious activity or encryption detected
- IT/security team confirms potential ransomware
- Executive leadership notified
- Incident response process activated

**5-15 Minutes**



### Containment Begins

- Identify potentially infected systems
- Isolate affected hosts from the network
- Disable compromised credentials
- Limit lateral movement across systems

**15-30 Minutes**



### Executive Decision Preparation

- Confirm scope of affected systems
- Determine if backups are intact
- Assess whether sensitive data may be exposed
- Engage cybersecurity incident response team

**30-60 Minutes**



### Strategic Response Activation

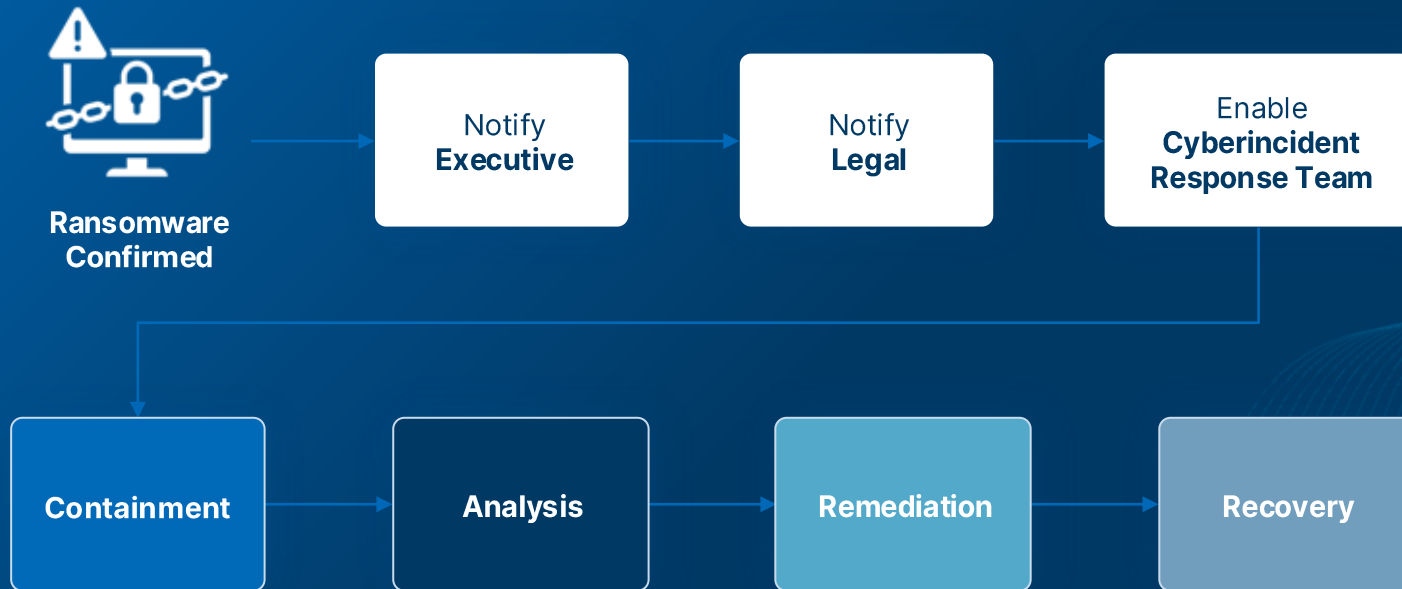
- Notify cyber insurance provider
- Engage legal counsel if regulated data may be involved
- Begin forensic investigation
- Prepare internal communication plan

# The Ransomware Response Framework

Every ransomware incident moves through four core phases:



# Ransomware Response Flow



## PHASE 1

# Containment

## Objective

Stop the ransomware from spreading.

## Key Actions

- ✓ **Identify** infected systems
- ✓ **Isolate** affected hosts
- ✓ **Reset** compromised credentials
- ✓ **Limit** lateral movement across the network

Identify affected hosts



Isolate affected hosts



Reset impacted user/host credentials



**ANALYSIS**



**Rapid containment can dramatically reduce operational damage**

## PHASE 2

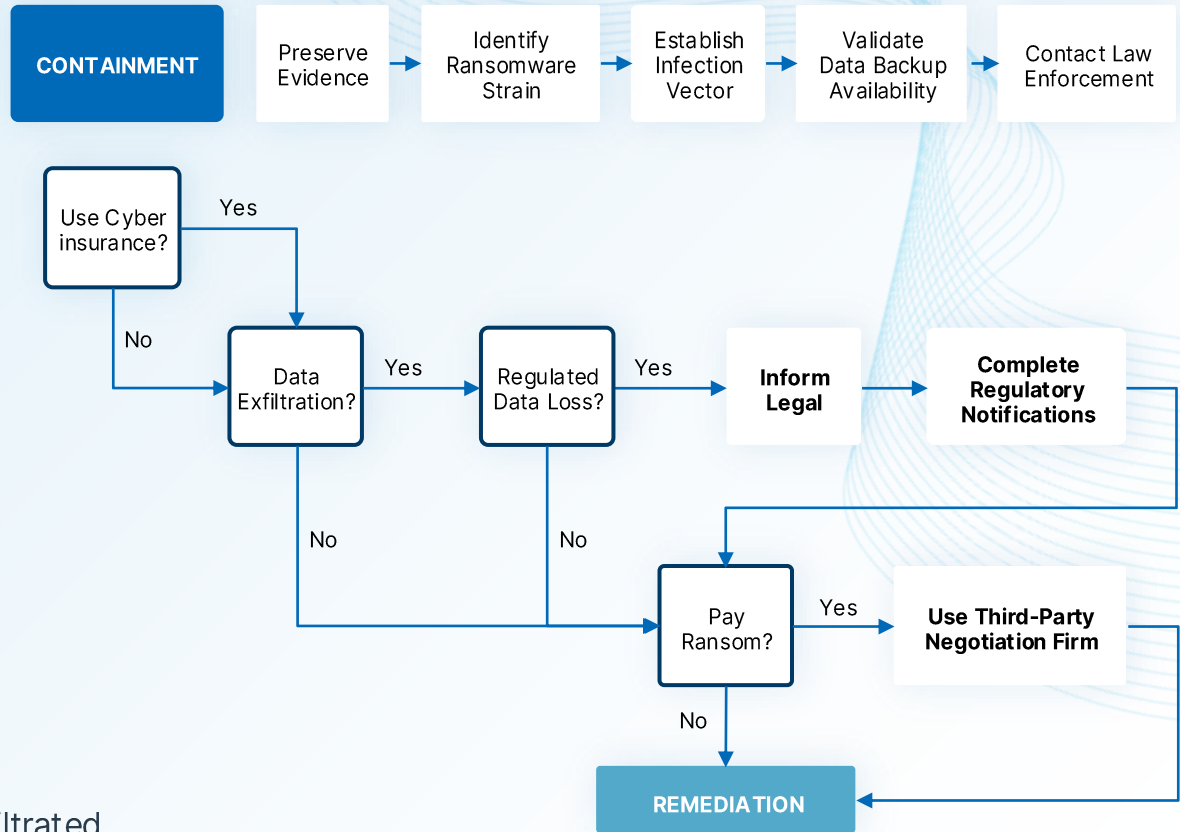
# Analysis

## Objective

Understand the attack.

## Key Actions

- ✓ **Preserve** forensic evidence
- ✓ **Identify** ransomware strain
- ✓ **Determine** infection vector
- ✓ **Assess** scope of compromise
- ✓ **Confirm** whether data was exfiltrated



## PHASE 3

# Remediation

## Objective

Remove the attacker's presence.

## Key Actions

- ✓ **Run** full malware scans
- ✓ **Remove** malicious artifacts
- ✓ **Patch** exploited vulnerabilities
- ✓ **Update** threat detection systems
- ✓ **Add** indicators of compromise to detection platforms

## ANALYSIS

Add IoC to threat platform

Run full antivirus anti-malware scan

Submit samples to vendors

## RECOVERY

## PHASE 4

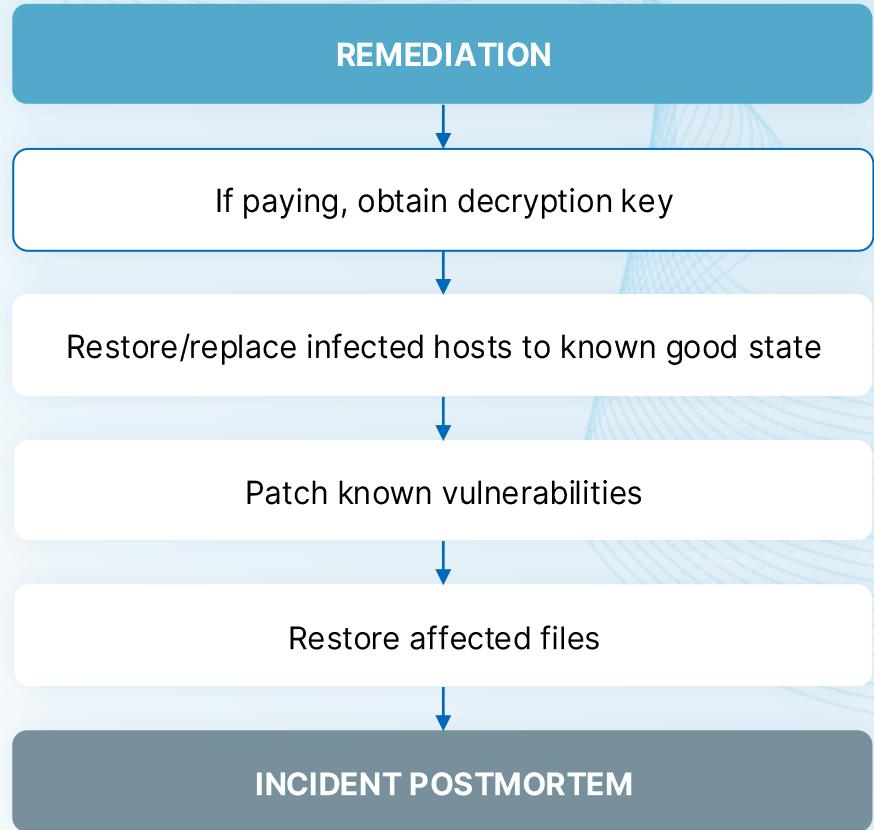
# Recovery

## Objective

Restore operations safely.

## Key Actions

- ✓ **Restore** systems from known good backups
- ✓ **Rebuild** compromised infrastructure
- ✓ **Apply** security patches
- ✓ **Validate** restored systems
- ✓ **Prioritize** restoration of critical business systems



# How a Typical Ransomware Attack Unfolds



Initial  
Compromise



Lateral  
Movement



Data  
Exfiltration



Encryption  
Event




Ransom  
Demand



Operational  
Recovery

# Critical Decision Points During an Attack

## Key leadership decisions:

-  Engage cyber insurance
-  Notify law enforcement
-  Determine scope of data exposure
-  Assess regulatory notification requirements
-  Decide whether to negotiate ransom



Many of these decisions must occur **within hours** of detection.

# The Business Cost of Ransomware

Industry statistics averages:

**\$1M**

Ransomware Recovery Cost

**21+ days**

Operational downtime

**\$200K**

Ransom Demand

**3-6 weeks**

Recovery Time

# Ransomware Readiness Checklist



Organizations should ensure they have:

Documented incident response plan

Defined cybersecurity response team

Verified backup strategy

Endpoint detection and monitoring

Legal and cyber insurance contacts

Defined executive decision process

# The Most Common Preparedness Gaps

Many mid-market organizations discover gaps only after an incident.

## Typical gaps include:

- ⊗ Unverified backups
- ⊗ Incomplete incident response plans
- ⊗ Unclear decision authority
- ⊗ Limited threat monitoring
- ⊗ Delayed executive communication

# How Prepared Is Your Organization?

Many companies assume they are ready for ransomware until they test their response process.

**A ransomware readiness review evaluates:**



Incident response planning



Security monitoring



Backup recovery capabilities



Regulatory preparedness

# Schedule a Ransomware Readiness Assessment

Our security specialists will help evaluate:

 Ransomware response preparedness

 Backup and recovery capabilities

 Incident response planning

 Cybersecurity monitoring

[Schedule Your Strategy Session !\[\]\(6204b2b9447b1eb7bc3c04a584718a35\_img.jpg\)](#)

# About Entech

Entech helps mid-market organizations align technology, cybersecurity, and operations to support business performance.

## Services:

- ✓ Managed IT Services
- ✓ Managed Cybersecurity
- ✓ Compliance and Risk Management
- ✓ Strategic IT Advisory



Serving Florida  
For more than  
25 Years