First 72 Hours of a Ransomware Event

In a ransomware event, the first 72 hours set the trajectory for everything that follows. Fast containment, informed decisions and coordinated expertise can limit downtime.

Hours 0-24
Incident Confirmation & Immediate Containment

- **Ransomware incident confirmed**
- **Impacted systems isolated from the internet to contain further threat actor actions.**
- **Cyber insurance carrier notified** Carrier introduces incident response counsel and forensic firm to develop a plan of action to identify the following:
  - Known impacted systems including need for third-party recovery teams
  - Immediate business disruptions
  - Initial containment actions underway
  - Internal and external communications needs and plans

Key Executive Decisions

Approve engagement of external incident response and legal support

Hours 24-36
Scope, Impact, and Exposure Assessment

- **Recovery progresses working closely with forensic team**
  - Evidence preserved during restoration of systems
  - Security tools deployed before access to the internet is restored
  - Evaluation of need for backups and/or decryption tool
  - Evaluation of backups for integrity and restorability
- **Forensic investigation begins to determine:**
  - Entry point and affected systems
  - Whether data exfiltration occurred
- **Business impact assessment initiated:**
  - Critical services affected
  - Operational and customer impact
- **Privacy counsel evaluates:**
  - Regulatory notification requirements
  - Contractual notice obligations to partners or clients
- **Controlled internal communications are considered**
- **Throughout the claim process, the Great American adjuster remains actively engaged to support vendor approvals, statements of work, and to help identify any additional coverage that may be available.**

Key Executive Decisions

Evaluate need for acquiring a decryption key and assess potential data at risk

With the right expertise and a clear plan, businesses can contain the threat quickly and move toward recovery with fewer surprises.

Hours 36-48
Strategy Alignment and Recovery Planning

- Threat actor profile and ransomware strain assessed
- Monitoring enhanced to detect persistence or lateral movement
- Restoration strategy developed:
  - Prioritized system recovery
  - Credential resets and security hardening
- Threat actor communications typically begin (handled by counsel/IR firm)
- Counsel reports to appropriate law enforcement agency(ies)
- Begin to analyze suspected data impact
- Analyze potential business downtime
- Counsel reviews regulatory and legal exposure

Key Executive Decisions

Approve phased restoration plan Determine whether additional remote/onsite resources are necessary

Determine posture on threat actor engagement (if applicable)

Hours 48-72
Restoration, Compliance, and Reputation Management

- Phased system restoration underway for priority services
- Continuous validation to ensure no reinfection
- Notification timeline analysis (state, federal, contractual)
- Counsel assists with internal/external communications if warranted

Deliverables
by Hour 72

Stable environment with strategy for recovery

Initial assessment of potential legal and regulatory obligations

Unified communication strategy

GREAT AMERICAN INSURANCE GROUP | Cyber Risk