

Incident response checklist

A quick reference for your incident lead: establish control, limit the impact, preserve evidence, and recover with a plan.

Use your organization's response plan and qualified responders. Protect life and essential services first; coordinate changes to operational or safety-critical systems with their operators.

☐ 01 Activate your response team

Name an incident lead. Use a trusted phone or other channel outside affected systems. Bring in your technical responders and notify the appropriate leadership and insurer contacts.

☐ 02 Contain affected systems

Coordinate isolation of affected IT devices or networks. Keep devices powered on where safe to preserve volatile evidence. If isolation is impossible and ransomware is spreading, responders may need to power them down.

☐ 03 Record and preserve evidence

Record times and time zones, affected assets, alerts, and actions taken. Preserve relevant logs, messages, and system evidence. Avoid wiping, reimaging, or deleting files before responders capture what they need.

☐ 04 Assess the scope and impact

Identify affected services, accounts, data, and dependencies. Separate confirmed facts from assumptions. Reassess containment as responders learn more about the incident.

☐ 05 Secure access and recovery assets

Have responders address compromised accounts and sessions from a known-clean device. Protect backups and their administration paths. Preserve clean recovery copies before making changes.

☐ 06 Coordinate communications

Agree on one source of status updates. Work with leadership, counsel, and your insurer to determine notifications and reporting to authorities. Share approved facts through trusted channels.

☐ 07 Restore in a controlled sequence

Have responders validate containment and address the entry path before reconnecting systems. Restore from known-good sources, verify essential services, and monitor closely for renewed activity.

☐ 08 Capture lessons and assign owners

Document the timeline, decisions, and recovery results. Assign owners and dates to improvements. Update your response plan and exercise the changes.

Incident lead: _____ Detected (date / time / zone): _____

Critical services affected: _____

Incident response: 888-438-1168 | info@karhucyber.com

Call to discuss availability. Use a trusted device and communication channel.