AMERICAN
TECHNOLOGY
SERVICES

Incident Response Maintenance Checklist

What to Do After a Cybersecurity Incident

What Comes After Containment and How to Make the Most of It

You have made it through the crisis. Now comes the part too many teams skip: learning from what happened, reinforcing what worked, and fixing what did not. This checklist outlines the essential steps for post-incident recovery, reflection, and preparation, so the next response is stronger, faster, and possibly preventable.

Post-Incident Maintenance: From Response to Resilience

Check these off as you debrief, document, and build back stronger.

- ☐ **You have completed a full debrief with internal and external stakeholders.**
  Everyone needs clarity before details fade: what happened, how it unfolded, what worked, and what did not.

- ☐ **You've reviewed and updated your incident response plan.**
  Real-world events should shape how you prepare for the next one. What changed? What needs to?

- ☐ **You have documented the full timeline, scope, and resolution.**
  Every step from detection to containment should be captured in detail. This creates a reliable audit trail and strengthens your legal and regulatory position.

- ☐ **You have validated the fixes and confirmed that attacker access is closed.**
  Do not assume it is over. Confirm that vulnerabilities are patched, persistence mechanisms are removed, and accounts are secured.

- ☐ **You have followed up on strategic remediation recommendations.**
  Focus on more than quick fixes. Address the systemic issues and resolve the root causes, not just the symptoms.

- ☐ **You've scheduled a retest or validation assessment.**
  If external support was used, confirm the cleanup. If internal, plan a sanity check. Recovery without validation is just hope.

- ☐ **You've documented lessons learned and shared them appropriately.**
  What can your broader org or leadership take away from this? Transparency builds trust.

- ☐ **You have set a cadence for testing, drills, and incident response plan reviews.**
  Maintenance depends on consistency. Do not wait for the next crisis; train, test, and review regularly.

What This Means

An incident does not end when the attacker is gone. It ends when your systems are secured, your people are aligned, and your process has improved. ATS helps you move from reaction to resilience without losing momentum.

The best response is one you don't need to repeat. Let's make sure of that.

info@networkats.com