Basic Incident Response Checklist

Ethos Technology & Cybersecurity · etc-advisors.com · ER@etc-advisors.com · 712-499-8769

Print this page and keep it accessible — physically, not only on the device that may be compromised. The first hour matters more than almost anything that follows.

DO

- [ ] REMAIN CALM
- [ ] Contact your leadership chain of command
- [ ] Contact cybersecurity professional, cyber insurance provider or legal counsel first
- [ ] Note where each network cable was connected, or take a picture, before unplugging
- [ ] Disconnect network (ethernet) cable from firewall
- [ ] Disconnect network (ethernet) cables or turn off Wi-Fi from affected devices
- [ ] Disconnect network (ethernet) cables to stop Bad Actors from getting access or extracting data
- [ ] Check whether backups are intact and isolated
- [ ] Log the exact time and what was observed
- [ ] Consult with counsel before reporting to law enforcement
- [ ] KEEP ALL DETAILS CONFIDENTIAL. Notify staff not to disclose details with family, friends, or social media.

DO NOT

- [ ] DO NOT Power off affected machines
- [ ] DO NOT Unplug power cables. Only disconnect network cables
- [ ] DO NOT Delete or wipe anything
- [ ] DO NOT Pay the ransom on impulse
- [ ] DO NOT Contact or respond to the threat actor yourself
- [ ] DO NOT Reinstall or reimage systems immediately
- [ ] DO NOT Restore from backup before the environment is contained

First Hour Checklist

- [ ] **1. Disconnect**
  Disconnect network cable of affected devices from the network and internet. Disconnect ONLY network (ethernet) cables — not power cables — to stop Bad Actors from accessing or extracting data. Note where each network cable was connected, or take a picture, before unplugging.
- [ ] **2. Contact**
  Your first contact should be your cybersecurity professional and your cyber insurance provider or legal counsel — before any other action is taken.
- [ ] **3. Do Not Engage**
  Do not contact or respond to the threat actor yourself. If contact is made, it should only be handled by your cybersecurity professional, and only after consulting counsel.
- [ ] **4. Preserve**
  Do not delete, wipe, or reinstall anything. Photograph ransom notes exactly as they appear. Log the exact time of discovery and what was observed.
- [ ] **5. Assess Backups**
  Check whether backups are intact and isolated from the compromised environment. Do not restore yet.
- [ ] **6. Report**
  Consult with counsel first. Report to law enforcement (FBI IC3) only after that conversation has taken place.

Basic Incident Response Checklist

Ethos Technology & Cybersecurity · etc-advisors.com · ER@etc-advisors.com · 712-499-8769

Key Contacts

Fill this in now, before an incident happens, so it is ready when you need it.

YOUR CYBERSECURITY PROFESSIONAL

Ethos Technology & Cybersecurity

Phone: 712-499-8769 Website: etc-advisors.com

Email: ER@etc-advisors.com

Cyber Insurance Provider

Name / Firm _____ Policy Number _____ Phone _____ Email _____

Policy Holder / Authorized Users to Contact Insurer _____

Legal Counsel

Name / Firm _____ Phone _____ Email _____

Internal Point of Contact / Chain of Command

Name / Firm _____ Phone _____ Email _____

Incident Log

Record what was seen and when — as it happens. This matters for investigation, insurance, and legal follow-up.

Date / Time	What Was Observed