

FREE RESOURCE

Cyber Incident First-Response Checklist

A practical, step-by-step guide for the first minutes and hours after detecting a cyber incident. Use it to protect people, preserve evidence, reduce business impact and coordinate a controlled response.

Important: Use this checklist alongside your incident response plan, legal advice, cyber insurance requirements and instructions from qualified responders. Do not perform forensic collection or destructive remediation unless you are authorised and trained.

1. First 15 Minutes: Stabilise and Take Control

- ☐ **Protect people first.** If the incident creates a physical safety risk, call emergency services and follow site safety procedures.
- ☐ **Record the detection time.** Note who reported it, how it was detected and the timezone used.
- ☐ **Assign an incident lead and a scribe.** One person coordinates decisions; another records every action and timestamp.
- ☐ **Open an incident log.** Use a separate, access-controlled document or approved case-management system.
- ☐ **Preserve the scene.** Do not delete files, wipe devices, reinstall systems or run "cleanup" tools before evidence is considered.
- ☐ **Isolate active threats carefully.** For a suspected infected workstation, disconnect network cables and Wi-Fi while leaving the device powered on, unless there is a safety risk or your responder instructs otherwise.
- ☐ **Use a known-clean device.** For email, cloud or privileged-account compromise, coordinate session revocation and credential changes from a trusted system.
- ☐ **Capture what you can see.** Save screenshots or photos of alerts, ransom notes, unusual messages, error screens and affected applications.
- ☐ **Activate the response team.** Notify security/IT, executive leadership, legal/privacy, cyber insurer and specialist responders according to your plan.
- ☐ **Set an initial severity level.** Reassess as new facts emerge.

Quick severity guide

Level	Typical indicators	Immediate action
Critical	Active ransomware, major outage, privileged account compromise, confirmed data theft, safety impact.	Activate executive, legal, insurer and specialist incident response support immediately.
High	Multiple systems affected, suspected lateral movement, sensitive data exposure, production disruption.	Formal incident bridge, rapid containment and evidence preservation.
Medium	Single account or device affected, limited scope, no confirmed sensitive data loss.	Investigate promptly, contain, document and monitor for escalation.

2. Collect and Preserve Evidence

Preserve enough information to understand what happened, when it started, what was affected and whether the attacker still has access.

- ☐ **Identify each affected asset:** hostname, username, IP address, device type, operating system, physical or cloud location and business owner.
- ☐ **Record accurate timestamps and timezone.** Note whether system clocks appear incorrect or unsynchronised.
- ☐ **Save original suspicious emails.** Preserve the full message and headers, preferably as an .eml or .msg file. Do not rely only on screenshots.
- ☐ **Export relevant logs.** Include EDR, SIEM, identity, VPN, firewall, email, cloud, DNS, web proxy, application and authentication logs.
- ☐ **Preserve alerts and case data.** Export detections before retention limits, automatic cleanup or account changes remove them.
- ☐ **Document visible indicators.** File names, hashes, domains, IP addresses, user accounts, process names, commands, persistence locations and ransom-note text.
- ☐ **Preserve volatile data when appropriate.** Memory, running processes and network connections should be collected by trained personnel using approved tools.
- ☐ **Create forensic images when required.** Disk or cloud snapshots should be taken by qualified responders and stored securely.
- ☐ **Maintain chain of custody.** Record who collected each item, when, how, from where and where it is stored.
- ☐ **Keep originals protected.** Work from verified copies; restrict access and avoid altering timestamps or metadata.
- ☐ **Preserve third-party evidence.** Ask hosting, SaaS, telecom and managed-service providers to retain logs before they expire.

Avoid accidental evidence loss: Do not forward malicious attachments broadly, repeatedly open suspicious links, delete attacker accounts before documenting them, or power off systems without responder guidance.

Incident Action Log

Time / timezone	Person	Action, observation or decision

3. Contain the Incident Without Destroying Evidence

- ☐ **Define the containment objective.** Decide whether the priority is stopping damage, preserving visibility, maintaining critical operations or a combination.
- ☐ **Isolate affected endpoints or network segments.** Use EDR isolation, switch controls, firewall rules or VLAN segmentation where available.
- ☐ **Disable or restrict compromised accounts.** Preserve account details first, then revoke active sessions, tokens, API keys and application passwords.
- ☐ **Block confirmed malicious indicators.** Apply carefully scoped controls for domains, IPs, hashes, sender addresses and URLs.
- ☐ **Protect privileged access.** Review administrator accounts, service accounts, remote access, federation, MFA changes and recently created credentials.
- ☐ **Secure backups.** Confirm that offline or immutable copies are protected from deletion, encryption and unauthorised access.
- ☐ **Stop exposed services where necessary.** Coordinate with business owners to reduce operational harm.
- ☐ **Monitor for attacker movement.** Look for new logins, persistence, privilege escalation, lateral movement and data staging.
- ☐ **Coordinate major actions.** Record approvals before broad shutdowns, mass password resets, domain-wide changes or public communications.

4. Communication and Notification

- ☐ **Use approved, trusted communication channels.** If corporate email or chat may be compromised, move the response team to an out-of-band channel.
- ☐ **Keep one source of truth.** Maintain a current incident summary, timeline, scope, decisions, owners and next update time.
- ☐ **Notify legal and privacy teams early.** They can assess contractual, regulatory, evidence and privilege requirements.
- ☐ **Contact the cyber insurer or broker promptly.** Follow policy conditions before appointing vendors, negotiators or making commitments.
- ☐ **Coordinate third-party notifications.** Inform customers, partners, regulators, law enforcement or vendors only through the authorised process.
- ☐ **Assign one spokesperson.** Employees should not post details, contact the media or speculate publicly.
- ☐ **Share facts, not assumptions.** Label unconfirmed information clearly and correct the record as evidence changes.

Potential notification triggers

Personal or payment data may be exposed; regulated systems are affected; critical services are unavailable; a third party may have access; contractual reporting deadlines apply; or law enforcement assistance may be appropriate.

5. Eradication and Secure Recovery

- ☐ **Confirm the initial access path.** Identify how the incident began and whether the entry point is still open.
- ☐ **Identify persistence and affected identities.** Review scheduled tasks, services, startup items, cloud apps, OAuth grants, keys, tokens and administrator changes.
- ☐ **Close the exploited weakness.** Patch vulnerabilities, correct misconfigurations and remove exposed services or credentials.
- ☐ **Rotate credentials in the right order.** Start with privileged, identity, backup and service accounts, using known-clean systems and a coordinated plan.
- ☐ **Rebuild compromised systems from trusted sources.** Prefer clean reinstallation or known-good images over unverified "cleaning."
- ☐ **Validate backups before restoration.** Check integrity, date, malware status, access controls and whether the backup predates compromise.
- ☐ **Restore in stages.** Prioritise critical services, isolate restored systems initially and monitor before wider reconnection.
- ☐ **Test business functions.** Confirm authentication, transactions, data integrity, integrations, logging and security controls.
- ☐ **Increase monitoring.** Watch for repeat indicators, suspicious authentication, new persistence and unusual data movement.
- ☐ **Keep evidence and response records.** Do not discard systems or logs until legal, insurer and investigation requirements are satisfied.

Before Declaring the Incident Resolved

- ☐ The incident scope and affected data are reasonably understood.
- ☐ Known attacker access, persistence and malicious infrastructure have been removed or blocked.
- ☐ Compromised credentials, tokens, keys and certificates have been rotated or revoked.
- ☐ Restored systems are patched, hardened, logged and monitored.
- ☐ Critical business processes and data integrity have been validated by owners.
- ☐ Required internal, contractual, legal, insurer and regulatory notifications are complete or scheduled.
- ☐ A heightened monitoring period, owner and end date are documented.

Recovery principle: Restoring service quickly matters, but reconnecting an unsafe system can restart the incident. Use staged recovery with clear go/no-go approval.

6. Post-Incident Review and Improvement

- ☐ **Build a verified timeline.** Include detection, attacker activity, decisions, containment, recovery and notifications.
- ☐ **Document root cause and contributing factors.** Separate confirmed facts from assumptions and unresolved questions.
- ☐ **Measure business impact.** Downtime, affected users, data exposure, operational loss, response cost and customer impact.
- ☐ **Review response performance.** What worked, what slowed the team and where authority or communication was unclear.
- ☐ **Track corrective actions.** Assign an owner, priority, deadline and evidence of completion for each improvement.
- ☐ **Update plans and exercises.** Revise playbooks, contact lists, training, monitoring, backup procedures and tabletop scenarios.

Common mistakes to avoid

- ☐ Wiping, reimaging or powering off systems before evidence and containment needs are assessed.
- ☐ Using a potentially compromised email account or device to coordinate the response.
- ☐ Resetting every password at once without protecting identity infrastructure and active sessions first.
- ☐ Failing to contact legal counsel, the cyber insurer or specialist responders early enough.
- ☐ Publishing unverified details or promising that no data was affected before the investigation supports it.
- ☐ Restoring from backups without confirming that the entry point and attacker persistence are removed.

Emergency Contact Worksheet

Complete this section before an incident and store the checklist in a location that remains available during an outage.

Incident response provider		
Cyber insurer / broker		
Legal counsel		
Executive incident lead		
IT / security lead		
Privacy / compliance lead		
Backup / recovery owner		
Critical technology vendor		
Law enforcement contact		

Document owner: _____ Last reviewed: _____

Need expert support? Fcreative Studio 360 helps organisations prepare for, respond to and recover from cyber incidents. Contact your account representative or visit www.fcreativestudio360.com.

Disclaimer: This resource provides general operational guidance and is not legal, regulatory, insurance or forensic advice. Requirements vary by jurisdiction, contract and incident type.