First 24 Hours

Cyber Incident Response Checklist | Free Download

The first 24 hours after discovering a cyber incident are critical. Every action taken—or not taken—during this window can significantly impact the scope of damage, your insurance coverage, regulatory obligations, and legal exposure. This checklist guides your response team through the essential steps, organized by time phase, to help you contain the threat, preserve evidence, and meet notification requirements.

IMPORTANT: Notify your cyber insurance carrier as early as possible. Most policies require prompt notice of any incident that may give rise to a claim. Failure to provide timely notice can jeopardize coverage. Contact First Underwriters at **(425) 242-5357** for immediate guidance.

Incident Information

Organization:		**Incident Date/Time:**	
Completed By:		**Role / Title:**	
Incident Type:		**Systems Affected:**	

Phase 1: Immediate Response (0–1 Hour)

These actions must be taken immediately upon discovery of a suspected cyber incident.

	Time	Action Item	Owner	Status / Notes
☐	0–15m	Confirm the incident is real (not a false alarm or test)	IT Lead	
☐	0–15m	Document the exact date, time, and method of discovery	IT Lead	
☐	0–15m	Identify the person who first discovered the incident	IT Lead	
☐	0–30m	Alert the internal incident response team leader	Discoverer	
☐	0–30m	Isolate affected systems from the network (do NOT power off)	IT Team	
☐	0–30m	Disable compromised user accounts and reset credentials	IT Team	
☐	30–60m	Preserve all logs, screenshots, and forensic evidence	IT Lead	
☐	30–60m	Begin an incident log documenting all actions and decisions	IR Lead	
☐	30–60m	Assess initial scope: what systems, data, and users are affected	IT Team	

Phase 2: Escalation & Notification (1–4 Hours)

Escalate to leadership, legal, and insurance. Begin formal notifications as required.

	Time	Action Item	Owner	Status / Notes
☐	1–2h	Notify executive leadership / CEO / business owner	IR Lead	
☐	1–2h	Contact cyber insurance broker (First Underwriters: 425-242-5357)	IR Lead	
☐	1–2h	Contact cyber insurance carrier claims hotline	IR Lead	
☐	1–2h	Engage legal counsel experienced in data breach response	IR Lead	
☐	2–4h	Engage approved forensic investigation provider	Legal / IT	
☐	2–4h	Determine if law enforcement notification is warranted	Legal	
☐	2–4h	Assess whether personal data or PHI/PII was exposed	Legal / IT	
☐	2–4h	Identify regulatory notification obligations (state, federal, HIPAA)	Legal	
☐	2–4h	Brief the communications / PR team on messaging hold	IR Lead	

Phase 3: Containment & Investigation (4–12 Hours)

Focus on stopping the spread, understanding the attack vector, and preserving evidence for forensics.

	Time	Action Item	Owner	Status / Notes
☐	4–6h	Confirm all affected systems are isolated and contained	IT Team	
☐	4–6h	Identify the attack vector (phishing, vulnerability, credential theft, etc.)	Forensics	
☐	4–6h	Determine if the attacker still has active access	Forensics	
☐	4–6h	Secure and image affected systems for forensic analysis	Forensics	
☐	6–12h	Assess the extent of data accessed, exfiltrated, or encrypted	Forensics	
☐	6–12h	Identify any lateral movement within the network	IT / Forensics	
☐	6–12h	Verify backup integrity (confirm backups are not compromised)	IT Team	
☐	6–12h	Patch or remediate the exploited vulnerability if identified	IT Team	
☐	6–12h	Update the incident log with all findings to this point	IR Lead	

Phase 4: Communication & Compliance (12–18 Hours)

Coordinate internal and external communications. Address regulatory and contractual obligations.

	Time	Action Item	Owner	Status / Notes
☐	12–14h	Brief executive team on current status, scope, and next steps	IR Lead	
☐	12–14h	Coordinate with legal on notification obligations and timeline	Legal	
☐	12–14h	Prepare internal communication for employees (what to do / not do)	IR Lead	
☐	12–16h	Identify contractual notification requirements (clients, vendors)	Legal	
☐	12–16h	Determine if credit monitoring or identity protection is needed	Legal	
☐	14–18h	Draft external breach notification language (pending legal review)	Comms / Legal	
☐	14–18h	Prepare customer-facing FAQ if public disclosure is anticipated	Comms	
☐	14–18h	Coordinate with insurance carrier on approved vendors and costs	IR Lead	
☐	14–18h	Document all costs incurred for insurance claim purposes	Finance	

Phase 5: Recovery Planning & Documentation (18–24 Hours)

Begin planning the path to recovery while ensuring all actions and evidence are fully documented.

	Time	Action Item	Owner	Status / Notes
☐	18–20h	Develop a prioritized system restoration plan	IT Lead	
☐	18–20h	Confirm clean backups are available for critical systems	IT Team	
☐	18–20h	Establish enhanced monitoring on restored and unaffected systems	IT Team	
☐	20–22h	Begin restoring critical business systems from clean backups	IT Team	
☐	20–22h	Implement additional security controls to prevent re-entry	IT / Forensics	
☐	20–22h	Reset all passwords and enforce MFA across the organization	IT Team	
☐	22–24h	Conduct a 24-hour status briefing with all stakeholders	IR Lead	
☐	22–24h	Compile a complete incident report with timeline and evidence	IR Lead	
☐	22–24h	Submit initial claim documentation to cyber insurance carrier	IR Lead	
☐	24h	Schedule follow-up review for Day 2 and ongoing response	IR Lead	

Emergency Contact Directory

Complete this section in advance and keep copies accessible (printed and off-network).

Role / Vendor	Organization / Name	Phone	Email
Incident Response Lead			
IT Lead / CISO			
CEO / Business Owner			
Cyber Insurance Broker	**First Underwriters**	**(425) 242-5357**	
Cyber Insurance Carrier			
Legal Counsel (Breach)			
Forensic Investigator			
PR / Communications			
Law Enforcement Contact			
IT Managed Services (MSP)			
Backup Provider			

Key Reminders:
- **Do NOT** pay any ransom without consulting your insurance carrier and legal counsel first.
- **Do NOT** power off affected systems—isolate them from the network instead to preserve evidence.
- **Do NOT** communicate about the incident on potentially compromised channels (email, Slack, etc.).
- **Do NOT** attempt to negotiate directly with threat actors.
- **DO** document everything: timestamps, decisions, personnel involved, and costs incurred.
- **DO** keep a printed copy of this checklist and your contact directory accessible off-network.

Acknowledgment

This checklist has been reviewed and is accessible to all members of our incident response team.

Name	Title / Role	Signature	Date

Disclaimer
This checklist is provided by First Underwriters Insurance Brokers as a complimentary resource for informational and risk management purposes only. It does not constitute legal, technical, or professional advice. Every organization's IT environment and risk profile is unique; this checklist should be customized to fit your specific incident response plan. Completion does not guarantee insurance coverage or claim approval. Consult with your IT provider, legal counsel, and insurance broker.