Cyber Incident First-Hour Checklist

What to do in the first hour of a ransomware attack, data breach or other serious cyber incident. Decisions made early shape the whole recovery, so act fast but keep a record.

0 to 15 minutes: confirm and escalate	Done	Notes
Confirm the incident and alert the incident response lead.		
Start a time-stamped log of everything seen, decided and done.		
Switch to communication channels the attacker cannot see, such as phones or an out-of-band chat.		

15 to 30 minutes: contain	Done	Notes
Isolate affected systems from the network. Avoid powering them off, which can destroy evidence.		
Disable compromised accounts and reset privileged credentials.		
Protect backups: take them offline or confirm they are isolated.		

30 to 45 minutes: assess	Done	Notes
Establish what is affected: systems, services, data and locations.		
Identify whether personal data may be involved.		
Do not contact the attacker or pay a ransom without legal and expert advice.		

45 to 60 minutes: notify and plan	Done	Notes
Call your cyber insurer's incident line, if you have one, and bring in specialist support.		
Brief senior leadership and agree who decides what.		
Check notification duties. A personal data breach may need reporting to the data protection authority within 72 hours under GDPR, and sector rules such as NIS2 or DORA can apply shorter deadlines.		
Prepare a holding statement for staff and, if needed, customers.		
Set recovery priorities: which services must come back first.		

Have this checklist printed and stored offline. During an attack, your files and systems may be unavailable.

General guidance only. Adapt it to your organisation's own policies, procedures and legal or regulatory requirements before use.