Cyber & Data Breach Incident Readiness Checklist

This high-level, non-exhaustive checklist helps organisations do an initial gap analysis for their Cyber & Data Breach Incident Readiness. It is not a full compliance assessment, audit tool, or legal advice, and it may not cover all requirements for CTM or DPTM certification.

Use this as a starting point to identify potential gaps. For a more detailed review or formal audit preparation, you should seek professional advice or conduct a comprehensive assessment.

1. Governance & Preparation

- ☐ An incident response (IR) policy is documented, approved by management, and communicated.
- ☐ A cross-functional incident response team (IRT) is defined (IT, security, legal, HR, communications, business owners).
- ☐ Roles and responsibilities for incident handling are clearly documented.
- ☐ Contact list for IRT members is up to date (including after-hours contacts).
- ☐ External contacts are identified and documented (regulators, outside counsel, forensics, PR, key vendors).
- ☐ Incident severity levels and impact criteria are defined (e.g. low, medium, high, critical).
- ☐ A documented incident response plan or playbook exists (end-to-end process from detection to closure).
- ☐ Incident categories are defined (e.g. phishing, ransomware, data leak, lost device, insider threat).
- ☐ Key systems and data assets are identified and classified (e.g. personal data, confidential, critical systems).
- ☐ Backup and recovery strategy is documented and tested for critical systems.

2. Detection & Reporting

- ☐ Security tools are in place to detect suspicious activity (e.g. antivirus/EDR, SIEM, IDS/IPS, email security).

- [ ] Security alerts are monitored at defined intervals (24/7 or business hours).
- [ ] Users are trained on how to recognise and report suspected incidents or phishing emails.
- [ ] A simple and clearly communicated incident reporting channel exists (e.g. dedicated email, hotline, ticketing).
- [ ] Criteria are defined to distinguish between an event, an incident, and a data breach.
- [ ] Initial triage procedures are documented (what to check, who to inform, how to classify).

3. Containment & Initial Response

- [ ] Guidelines are defined for immediate containment actions (e.g. isolate endpoints, disable accounts, block IPs/domains).
- [ ] Procedures exist for dealing with ransomware or malware outbreaks (e.g. isolate network segments, use clean backups).
- [ ] Playbooks include steps to avoid destroying potential evidence (e.g. avoid reimaging before capture, preserve logs).
- [ ] Decision trees exist for whether to shut down systems, disconnect from network, or keep online for monitoring.
- [ ] A process exists to reset credentials and revoke access as needed (including privileged accounts).
- [ ] Documented checklist exists for initial response actions during the first 24 hours of a serious incident.

4. Investigation & Analysis

- [ ] Procedures exist for collecting and preserving digital evidence (e.g. disk images, memory, logs).
- [ ] Logs are centralised and retained for an appropriate period to support investigations.
- [ ] Capability (internal or external) exists for forensic analysis of systems and networks.

- [ ] The organisation can identify what data may have been accessed, altered, encrypted, or exfiltrated.
- [ ] Root cause analysis (RCA) process is defined (how the incident occurred, exploited vulnerability, control failures).
- [ ] A standard template for incident reports is in place (timeline, impact, actions taken, lessons learned).

5. Impact Assessment & Legal/Regulatory Obligations

- [ ] Criteria are defined to assess whether an incident qualifies as a data breach involving personal or confidential data.
- [ ] The organisation can determine which individuals, customers, or partners are affected by a breach.
- [ ] Legal and regulatory obligations for breach notification are identified (e.g. data protection regulator, sector regulator).
- [ ] Internal guidance exists for when to consult legal counsel regarding notification obligations and liabilities.
- [ ] There is a process to assess potential harm to individuals (e.g. identity theft, financial loss, humiliation).
- [ ] Decision-making responsibilities for notification (who approves, what is notified, by when) are clearly defined.

6. Notification & Communication

- [ ] Template notifications are prepared in advance for affected individuals (plain language, guidance on next steps).
- [ ] Template communications exist for regulators and authorities (facts, impact, remediation actions).
- [ ] Internal communication plan is defined (who needs to know, what is shared, how to avoid panic or misinformation).
- [ ] External communication plan is defined (media statements, key messages, spokesperson, Q&A guidance).
- [ ] Customer-facing teams (e.g. call centre, account managers) are briefed on how to respond to queries.

- [ ] Records of all notifications and communications are retained (who was notified, when, what was communicated).

7. Recovery & Restoration

- [ ] Documented recovery procedures exist for restoring systems and data from backups.
- [ ] Restored systems are verified as clean and secure before returning to production (e.g. patched, hardened).
- [ ] Business processes are prioritised for restoration based on criticality.
- [ ] Users are informed about system status, downtime, and expected recovery timelines.
- [ ] Monitoring is enhanced for a period after restoration to detect any recurrence or related activity.

8. Post-Incident Review & Lessons Learned

- [ ] Post-incident reviews are conducted for significant incidents within a defined timeframe.
- [ ] Root causes and contributing factors are documented and analysed.
- [ ] Corrective actions are identified, implemented, and tracked to closure.
- [ ] Policies, procedures, and controls are updated based on lessons learned.
- [ ] Incident statistics and trends are reported to management on a regular basis.
- [ ] Training, awareness, and technical controls are updated to address identified gaps.

9. Training, Awareness & Testing

- [ ] Regular security awareness training includes how to report incidents and suspected breaches.
- [ ] Targeted training is provided to the incident response team and key stakeholders (legal, HR, communications).
- [ ] Phishing simulations or similar campaigns are conducted to test user readiness.

- [ ] Tabletop exercises are run periodically to rehearse breach scenarios and decision-making.
- [ ] Technical response capabilities (e.g. backup restore, failover, log review) are tested periodically.

10. Third Parties & Outsourced Services

- [ ] Contracts with key vendors and service providers include incident reporting and cooperation obligations.
- [ ] Third-party incident response roles and responsibilities are clearly defined (e.g. MSP, cloud provider, SOC).
- [ ] There is a process to coordinate investigations and communication with third parties during a breach.
- [ ] Third parties provide timely access to relevant logs and evidence upon request.
- [ ] Third-party incidents that may affect the organisation are monitored and assessed for impact.

For assistance, contact:

Hari Krishnan, Managing Director
Apex Organisational Solutions | www.apexorganisationalsolutions.com | hari.krishnan@apexorganisationalsolutions.com