Are You Cyber-Ready?

A Practical Cyber Threat Readiness Checklist for UK Organisations

INNOVARO

1. Identity Theft Protection & Account Takeover Prevention

Identity compromise is now one of the primary entry points for phishing, ransomware and data breaches. This section assesses how well your organisation can **prevent, detect and respond to identity-based attacks**.

1.1 Credential Protection

- [ ] Strong password standards enforced across all systems
- [ ] Password reuse prevented across corporate services
- [ ] Password managers approved and encouraged
- [ ] Shared or generic accounts eliminated
- [ ] Service account credentials securely stored and rotated
- [ ] Default credentials removed from all systems and devices

---

1.2 Compromised Credential Monitoring

- [ ] Automated alerts for exposed usernames or passwords
- [ ] Coverage includes corporate, cloud and third-party services
- [ ] Clear process for validating and responding to credential leaks
- [ ] Credentials rotated immediately following exposure
- [ ] Identity compromise metrics tracked and reviewed

1.3 Compromised Credential Monitoring

- [ ] Multi-Factor Authentication enforced for all users
- [ ] MFA enforced for administrators, remote access and cloud services
- [ ] Phishing-resistant MFA used for high-risk accounts where possible
- [ ] Conditional access based on device, location or risk level
- [ ] Legacy authentication protocols disabled
- [ ] Adaptive authentication challenges triggered for risky sign-ins

1.4 Account Takeover (ATO) Detection

- [ ] Monitoring for abnormal login patterns
- [ ] Detection of impossible travel or unusual geolocation activity
- [ ] Alerts for excessive failed login attempts
- [ ] Brute-force and credential-stuffing protections enabled
- [ ] Detection of unusual session duration or activity spikes
- [ ] Automated containment actions for suspected ATO
- [ ] High-risk identity activity prioritised for investigation

---

1.5 Privileged Identity Protection

- [ ] Privileged accounts clearly identified and documented
- [ ] Privileged access restricted to named individuals
- [ ] Just-in-time or time-limited admin access enforced
- [ ] Privileged sessions monitored and logged
- [ ] Alerts for privilege escalation attempts
- [ ] Regular privileged access reviews conducted

1.6 User Behaviour & Identity Analytics

- [ ] Baseline user behaviour established
- [ ] Monitoring for unusual access to data or systems
- [ ] Alerts for abnormal downloads or data exfiltration
- [ ] Identity signals correlated with endpoint and network activity

---

1.7 Identity Incident Response

- [ ] Identity-related incidents included in the Incident Response Plan
- [ ] Clear ownership for identity security incidents
- [ ] Defined procedures for account lockout and recovery
- [ ] Rapid credential reset and token revocation processes
- [ ] Forensic investigation procedures documented
- [ ] Identity incidents included in post-incident reviews

1.8 Staff Awareness & Identity Hygiene

- [ ] Staff trained to recognise identity-based attacks
- [ ] Guidance provided on secure password practices
- [ ] Training includes MFA fatigue and push-bombing attacks
- [ ] Clear reporting process for suspected account compromise
- [ ] Regular refresher training delivered

1.9 Third-Party & Supply Chain Identity Risk

- [ ] Third-party access accounts clearly identified
- [ ] Supplier access restricted to minimum required privileges
- [ ] MFA enforced for third-party users
- [ ] Regular review of supplier and contractor access
- [ ] Immediate removal of access upon contract end

1.10 Identity Threat Detection & Response (ITDR) Maturity

- [ ] Identity security monitored continuously
- [ ] Identity alerts integrated into SOC workflows
- [ ] Automated response playbooks in place
- [ ] Identity telemetry retained for investigation and compliance
- [ ] Regular testing of identity attack scenarios
- [ ] Alerts for leaked or reused passwords
- [ ] Controls to detect account takeover attempts
- [ ] Conditional access policies based on risk, location or device
- [ ] Brute-force and credential-stuffing protections enabled
- [ ] User login behaviour monitored for anomalies
- [ ] High-risk sign-ins blocked or challenged
- [ ] Rapid credential reset and account recovery procedures defined
- [ ] Identity-related incidents included in the Incident Response Plan

2. Strategy, Governance & Risk Management

- [ ] Cyber security strategy aligned to business objectives
- [ ] Cyber risk discussed at board or senior management level
- [ ] Named individual accountable for cyber security
- [ ] Information security policies documented and reviewed annually
- [ ] Clear escalation paths and decision-making authority defined
- [ ] Cyber insurance in place and reviewed against current threat landscape
- [ ] Supplier and third-party cyber risk assessments performed
- [ ] Data classification scheme in place
- [ ] Regular risk assessments conducted and documented

3. Phishing & Social Engineering Defence

- [ ] Advanced email filtering and threat protection enabled
- [ ] SPF, DKIM and DMARC configured and monitored
- [ ] External email tagging enabled
- [ ] MFA enforced for email and cloud services
- [ ] Regular phishing simulations conducted
- [ ] Security awareness training delivered at least annually
- [ ] Staff trained to recognise business email compromise (BEC)
- [ ] Clear and simple process to report suspicious emails
- [ ] Reported phishing emails investigated and acted upon

4. Endpoint, Server & Device Security

- [ ] Endpoint Detection & Response (EDR/XDR) deployed
- [ ] Endpoints monitored continuously
- [ ] Anti-malware and exploit protection enabled
- [ ] Automatic patching for operating systems
- [ ] Application patching processes in place
- [ ] Unsupported or legacy systems identified
- [ ] Encryption enabled on laptops and mobile devices
- [ ] USB and removable media controls enforced
- [ ] Mobile Device Management (MDM) in place where required

5. Ransomware Resilience & Data Protection

- [ ] Regular backups of critical systems and data
- [ ] Offline or immutable backups maintained
- [ ] Backup scope covers cloud, SaaS and on-prem systems
- [ ] Backup restoration tested regularly
- [ ] Clear ransomware response procedures documented
- [ ] Network segmentation implemented
- [ ] Lateral movement controls in place
- [ ] File integrity monitoring enabled for critical systems

6. Network & Cloud Security

- [ ] Firewalls and network security devices correctly configured
- [ ] Secure remote access (VPN or zero-trust) enforced
- [ ] Network traffic monitored for suspicious activity
- [ ] Cloud security configurations reviewed regularly
- [ ] Logging enabled across cloud platforms
- [ ] Default credentials removed
- [ ] Secure configuration baselines applied
- [ ] Regular vulnerability scanning conducted

7. Insider Threat Management

- [ ] Role-based access enforced across systems
- [ ] User activity monitored for anomalous behaviour
- [ ] Alerts for excessive downloads or data access
- [ ] Acceptable use policies communicated to staff
- [ ] Data loss prevention (DLP) controls in place or planned
- [ ] Strong joiner, mover and leaver processes
- [ ] Access removed immediately upon employee exit
- [ ] HR and IT coordination formalised

8. Monitoring, Logging & Threat Detection

- [ ] Centralised logging across endpoints, servers and cloud
- [ ] Logs retained in line with compliance requirements
- [ ] Security alerts configured for high-risk events
- [ ] Threat intelligence feeds in use
- [ ] Continuous or 24/7 security monitoring in place
- [ ] Security Operations Centre (SOC) capability available
- [ ] Alerts triaged and responded to in defined timeframes

9. Incident Response, Legal & Compliance

- [ ] Incident Response Plan includes cyber-specific scenarios
- [ ] Table-top or live incident exercises conducted
- [ ] Legal and regulatory obligations documented
- [ ] ICO breach notification process defined
- [ ] Evidence preservation procedures in place
- [ ] Communication plans for staff, customers and suppliers
- [ ] Third-party forensic support identified in advance

10. Business Continuity & Recovery

- [ ] Business Impact Analysis completed
- [ ] Recovery Time Objectives (RTO) defined
- [ ] Recovery Point Objectives (RPO) defined
- [ ] Disaster Recovery plan documented and tested
- [ ] Critical suppliers included in continuity planning
- [ ] Post-incident reviews conducted
- [ ] Lessons learned fed back into security controls

INNOVARO

Get in touch

0800 2800 365

sales@innovarouk.com

57-61 Mortimer Street,
London W1W 8HS.

www.innovarouk.com