CAPSLOCK

Cyber culture and behavioural change

Service overview

The CAPSLOCK Cyber Culture & Behaviour Change Programme reduces cyber risk by addressing the people, behaviours, and leadership practices that affect the secure operation of cloud services.

The service delivers measurable, sustainable improvements beyond traditional awareness training.

Service description

The programme focuses on how individuals and teams understand, manage, and take responsibility for cyber risk in day-to-day work.

It supports leadership accountability, improves staff behaviours, and embeds security into organisational culture and decision-making.

What the service provides

Core service elements

Service element	Description	Output
Cyber culture baseline assessment	Assessment using staff surveys, leadership interviews, and incident insights.	Cyber culture baseline report with prioritised risks.
Leadership and management enablement	Support for leaders and managers to: • Understand cyber accountability • Make risk-based decisions • Reinforce secure behaviours	Leadership cyber accountability framework.

CAPSLOCK

Cyber culture and behavioural change

Behaviour-focused interventions	Targeted interventions addressing: • Phishing and social engineering behaviours • Secure data handling • Incident reporting confidence • Policy compliance in real workflows	Role-specific behaviour change activities.
Cultural reinforcement	Embedding change through: • Security champions • Micro-learning • Reinforcement and communications strategies	Sustainable reinforcement plan.
Measurement and improvement	Re-assessment against the original baseline.	Culture maturity improvement report.

Buyer outcomes

Reduced human-related cyber incidents	Improved incident reporting quality	Stronger accountability and ownership
Better alignment between policy and practice	Improved organisational resilience	Strengthened organisational security culture maturity

CAPSLOCK

Cyber culture and behavioural change

Delivery model

- Remote, on-site or hybrid delivery
- Flexible duration (4 weeks to 6+ months)
- Scalable across departments or organisations

Security and assurance

ISO/IEC 27001:2022	**Cyber Essentials Plus**	**UK GDPR Compliant**	**Minimal Data Handling**

Suitable for

- Organisations experiencing repeat cyber incidents
- Cloud programmes with behavioural risk
- Audit, assurance, or compliance improvement initiatives
- Large or distributed public sector workforces