Cyber Security
Defence Consultants

Cyber Security Consultancy

January 2026

G-Cloud 15 Service Description

Cyber Security Defence Consultants Limited
St John's Innovation Centre
Cowley Road
Cambridge
CB4 0WS
T: 01223 421577
W: cybersecuritydefence.co.uk

Security Awareness and Training

Cyber Security Defence Consultants

Table of Contents

1 Overview 4
2 Services 4
2.1 Security Awareness Training 4

1 OVERVIEW

Cyber Security Defence Consultant provides high-quality cyber security consultancy services. Our team has worked with organisations to achieve cybersecurity outcomes in various complex and diverse environments. Outcomes include achieving certification to a chosen standard, including Cyber Essentials and Cyber Essentials Plus.

We have developed and implemented information risk management processes that support the clients' governance model and implement controls that are targeted to treat specific defined and quantified risks.

This approach ensures that the level of security controls is in line with the context of the organisation, the risk appetite of the organisation and the level of cyber threat faced by that organisation.

Our consultants are experienced and qualified. Many of our team are former CLAS consultants with an up-to-date approach to effective and proportionate risk management. Our team hold qualifications including CISSP, CISM and ISO/IEC 27001 Lead Auditor and Lead Implementer.

Our cyber security consultancy engagement process aligns with the NCSC Certified Cyber Security Consultancy Standard, ensuring a high-quality client journey including agreed deliverables, transparent and regular reporting, defined escalation paths, suitably skilled and qualified resources and focused delivery.

2 SERVICES

2.1 Security Awareness and Training

Security awareness training plays a crucial role in educating employees and individuals about cybersecurity best practices, potential threats, and measures to protect themselves and organisations from cyber-attacks.

People are widely targeted by attackers either at random or specifically, and Cyber Security Defence Consultants provide training to raise awareness and develop skills to prevent attacks from occurring within organisations.

Attackers seek to exploit weaknesses in people's understanding of how they work. By providing people with information, insight, and awareness to identify potential pitfalls, such as phishing emails, scam websites or the tactics, techniques and procedures used by attackers, they are empowered to protect themselves and the organisation.

Successful security awareness training is the difference between those users that are weak and those being the first line of defence against security attacks.

We focus on emphasising the importance of strong, unique passwords and encouraging the use of password managers or multi-factor authentication (MFA) for added security.

Cyber Security Defence Consultants are experienced in providing security awareness training to the general user community, specific user groups, such as developers and to senior leadership.

Educating individuals about various social engineering techniques used by attackers, such as pretexting, baiting, and tailgating, to manipulate people into divulging sensitive information or granting unauthorised access.

We provide guidance on handling sensitive data securely, including proper encryption, secure storage, and safe disposal practices.

Training is targeted to ensure that it is relevant and accessible. We provide background information on the attack

types, why attackers act as they do and how to spot the giveaway signs that betray an attempted attack.

We offer best practice training for securing mobile devices, such as using secure WIFI connections, enabling device encryption, and being cautious when installing apps.

Our reports on awareness training and attainment by the users are used as evidence to support ISO/IEC27001 compliance or fulfilling legal and contractual requirements.

The training can be delivered through various methods, including webinars, instructor-led sessions, online courses, simulated phishing exercises, and awareness campaigns. Regular training and reinforcement are essential to keep security knowledge and vigilance high among employees and individuals.