

Cybersecurity Education, Awareness, Behaviors and Culture Change Service

G-Cloud 15





Table of Contents

1	Service Overview	3
2	Business Need	4
3	Our Approach.....	5
4	Buyer Responsibilities	6
5	Service Management	6
6	Protection of Data	6
7	On-boarding and Off-boarding	7
8	Skills and Knowledge Transfer	7
9	Partnerships/Alliances.....	7
10	Vendor Accreditations/Awards	7
11	Sub-contractors	8
12	Business Continuity and Disaster Recovery	8
13	Pricing	9
14	Ordering and Invoicing	9
15	Termination Terms	9
16	Further Information	9



1 Service Overview

A robust Cybersecurity Awareness, Behaviours and Culture programme is essential for achieving a mature security posture and the effective management of human risk. In the constantly evolving realm of cyber threats, technical controls cannot offer complete protection, with human risk often exposing organisations to some of the most significant threats. Everybody must be aligned with management objectives and risk appetite.

Organisations are now required to navigate a landscape where cybercriminals benefit from advancements in technology, such as Artificial Intelligence and increased use of Cloud technologies due to the shift to hybrid working, allowing them to constantly adapt their tactics to exploit vulnerabilities in the workforce or supply chain. This is in addition to the ongoing risk of malicious insider threat and human error.

By nurturing a culture of security consciousness, organisations can empower their employees to become the first line of defence against cyber threats as opposed to a point of vulnerability. To achieve this, organisations should start deploying socio-behavioural principles to influence security culture in addition to awareness activities and campaigns. This involves integrating a deeper understanding of human behaviours and social dynamics into organisations' cybersecurity strategy, delving into the psychology and social aspects that influence how employees interact with technology.

This strategic move acknowledges the importance of both technological and human factors in securing an organisation.

Capgemini can help address these risks and challenges and deliver wide-spread benefits with an award-winning Cyber Awareness, Behaviour and Culture service (Best Culture Transformation winner at the 2025 Change Awards). It is comprised of one or more of the following aspects:

Leveraging Cloud-based technology: Several benefits can be gained from correctly leveraging cloud-based technologies and Capgemini is well positioned to support this based on experience in delivering Cybersecurity Awareness, Behaviour and Culture change paired with our wealth of Cloud technology experts. These benefits include but are not limited to; cost-effectiveness with regards to implementing solutions by removing the need to invest in infrastructure, and scalability allowing for the increase and/or decrease of service depending on workforce size or training needs.

- **Discovery:** Undertaking an assessment of the current maturity of Cyber Awareness, Behaviour and Culture to tailor the future approach and determine baseline levels of awareness. Based on requirements this can be conducted through one or more of the following components: interviews, workshops, assessment of relevant materials, data and metrics review and the implementation and delivery of a cybersecurity culture survey.
- **Strategy and Operating Model:** Creation of a Cyber Awareness, Behaviour and Culture strategy, operating model and roadmap to create a clear vision with buy-in at all levels, and which allows the strategic development of secure behaviours throughout the Buyer's organisation.
- **Data and Analytics:** Sourcing and analysing quantitative measures of behaviour alongside contributing cultural factors to support decision making, measure the efficacy of the activities, and to highlight key trends and performance to leaders.
- **Transformation:** Drive the transformation of the security behaviours and culture, underpinned by the strategy including the delivery of campaigns, interventions, feedback and continuous improvement. Help develop and promote a culture of continual engagement and feedback with staff to reinforce behaviour change over time by simplifying security and reducing friction for end users.
- **Behavioural Interventions:** To demonstrably reduce cybersecurity risk by establishing and maintaining positive behaviours through targeted and measurable interventions. A proven methodology will be applied to model, design, test and scale interventions.
- **Cybersecurity Culture Survey:** The design and development of a survey to help determine current and future cybersecurity culture. The survey and its outputs can act as a tracking tool to monitor awareness, behaviour and culture activities and will provide insights to inform decision making and future priorities.



- **Branding:** The development of creative concepts and a visual language for the programme which is in-line with organisational values and branding to resonate with the audience.
- **Campaigns:** Improving the baseline level of maturity amongst employees through delivering structured training and integrating awareness campaigns into daily life through targeted security briefings, webinars and seminars, Computer-Based Training (CBT), and themed campaigns delivered through a variety of media (such as posters, desk aids, games, videos, email, intranet and newsletters), targeted role-related briefing sessions, events and road shows
- **Security Induction:** Develop induction content, implement the security induction process into wider induction activities and track compliance to help security messages be embedded at the beginning of the employee lifecycle.
- **Phishing:** Delivery of phishing campaigns, monitoring associated data and metrics for analysis to tailor future campaigns and interventions.
- **Security Champions:** Creation of a Security Champions network, fostering a sense of community around Cybersecurity and normalising secure behaviours to embed security as a personal responsibility for all staff.

Crisis Exercises: Running simulations and exercises to practice responding to security incidents, promoting experiential learning from board level to operational level.

Chatbots and Digital: Maximising the effectiveness of security education and awareness by transforming underpinning organisational capabilities, including a staff-centric intranet website, a security advice helpdesk, an awareness demand management process, and a security chatbot built on Artificial Intelligence (AI). The integration of generative AI technologies facilitates employee upskilling, enables the extraction of critical security insights, and streamlines operational processes, collectively driving greater efficiency and mitigating organisational risk exposure.

- **Emerging Risks and Trends:** Acknowledging the change in attack surface as a result of the shift to hybrid working where office and remote working produce different risks, such as the increased reliance on Cloud hosted services like VPN's, content will be tailored accordingly.
- **Gamified learning:** equips security professionals with immersive, challenge-based training that mirrors real-world threats. By integrating game mechanics, it enhances engagement, sharpens critical thinking, and reinforces cybersecurity skills in a dynamic, risk-free environment.
- **Security Professionalization:** A framework designed to identify the Cyber skills and capability expected of professionals in the performance of their roles, thereby identifying the security skills required to support the professionalization of Cyber roles in their relevant profession.
- **Multidisciplinary Skillset:** This service leverages the collective skillset and varied experience within the award-winning Capgemini Security team. Capgemini consultants can make use of both their experience delivering awareness, behavioural and culture change as well as their technical knowledge spanning the Cybersecurity spectrum to deliver specific elements of the programme roadmap and facilitate knowledge sharing.

This service can be completely customised to the risk profile and threat vectors associated with the Buyer's organisation, and relates to both Cloud, On-Premise and Hybrid organisations. In all instances Capgemini will work with the Buyer's organisation to build a strong understanding of the "as-is" view of the organisation, with outputs then tailored accordingly.

2 Business Need

Organisations face challenges in keeping their Cybersecurity Awareness, Behaviour and Culture activities innovative, engaging, and effective. A traditional approach to cybersecurity awareness, behaviour and culture



may leave organisations vulnerable to increasingly sophisticated threats faced by all employees, regardless of role or seniority. Examples of this include:

- Traditionally relying on a “one size fits all” approach to training modules or content, lacking personalisation for specific job roles and emerging threats.
- Focusing on repetitive and sometimes technical topics within cybersecurity.
- Neglecting the human risk element of cybersecurity.
- Content having a long refresh cycle, with this static nature causing content to become outdated quickly.
- Inability to effectively track, report and glean actionable insights from cybersecurity awareness, behaviour and culture activities.

Capgemini’s Awareness, Behaviour and Culture service tackles these issues on behalf of organisations. Examples of this include:

- **Innovation:** exploring novel ways to deliver content, making use of the latest technology such as AI and Virtual Reality (VR).
- **Personalisation:** tailoring content for maximum engagement by making material relevant to individuals, their roles, and their responsibilities.
- **Trend monitoring:** factoring in the latest technological trends and their associated risks, and contextualising these in relation to the Buyer’s organisation.
- **Social:** People are influenced by the behaviours and attitudes they see around them. Socio-behavioural tactics leverage this to normalise secure behaviours. Examples include using quizzes and challenges with incentives such as recognition amongst the team (as determined by the Buyer’s organisation’s operating culture).

Additionally, regulatory requirements and compliance standards are increasingly mandating strong cybersecurity controls, making a mature awareness programme essential for compliance purposes. We can support compliance with cybersecurity standards (PCI DSS, ISO27001, HMG Infosec).

Capgemini has over 500 security professionals in the UK who can help deliver this service. This can incorporate consultants certified against CESG’s Certified Professional (CCP) scheme.

3 Our Approach

Capgemini’s approach is structured to allow for adaptation to the Buyer’s organisation and the agreed level of duration and complexity of the engagement. For all Cybersecurity Awareness, Behaviour and Culture services, Capgemini will follow best practice and frameworks, including but not limited to ITIL, TOGAF, ISO2700 along with the UPM and Prince2 project management frameworks.

Before the Cybersecurity Awareness, Behaviours and Culture service can be implemented, Capgemini consultants would collaborate with the Buyer’s organisation to understand any existing elements of the Buyer’s security strategy and wider business strategy relevant to the service delivery.

When delivering an end-to-end transformation of security behaviours and culture within the Buyer’s organisation, initial activities typically involve discovering the current maturity of cybersecurity awareness, behaviour and culture within the organisation, including the approach and tooling/software via workshops with the business, IT and Security stakeholders and documentation review.



This is followed by the Design phase where a roadmap including behavioural interventions, campaigns, culture surveys, training and strategic objectives are identified. The output of the Design phase then acts as the foundation for the Piloting phase, where some proposed activities are piloted to measure their impact and effectiveness, gaining insight to continuously improve and evolve the roadmap. This results in a final roadmap of activities to allow for the end-to-end transformation of security behaviours and culture of the Buyer's organisation.

Furthermore, Capgemini can provide dedicated awareness and training around priority topics. These topics can be identified by the Buyer's organisation directly or through discussing key trends across industries with Capgemini's experts. These priority topics could include regulatory requirements (such as GDPR), or technological trends (such as AI, Generative AI and Cloud Security).

Delivery of targeted awareness and training around priority topics can help employees understand their responsibilities, making security relevant to their role. Tailoring these topics also allows for:

- The Buyer's organisations business requirements to determine the course specification.
- Identification and compilation of course material from Buyer's existing training material and Capgemini's library of collateral.
- Scheduling & delivery of awareness training in line with the Buyer's organisations priorities i.e., a focus on induction and role-specific refresher training, or a focus on key topics

Assessment of existing tooling to deliver targeted training can form part of the defined roadmap. Where it is deemed suitable, the existing tooling may be enhanced and/or extended to meet the new requirements.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The Buyer responsibilities as part of this service are as follows:

- The Buyer will provide a project/engagement manager to act as a single point of contact and an escalation route for the full duration of the project/engagement.
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date.

If these responsibilities do not match your expectations, then please contact us in order that we can explore options to vary our approach.

5 Service Management

Capgemini can deliver the service as a defined programme of activity forming part of a wider Cybersecurity transformation or organisational change programme; a handover of business-as-usual activities to Buyer's staff forming part of the programme in this instance. Alternatively, it can be delivered as an ongoing business service run as a partnership between Capgemini and Buyer's organisation.

Whichever delivery model you choose, Capgemini can deliver the service with a particular emphasis on accountability and improvement.

6 Protection of Data



This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss. Our approach would be compliant with requirements of GDPR where applicable.

7 On-boarding and Off-boarding

Prior to the execution of the Order, the Supplier and the Buyer will agree the scope of the exit plan for the Services and a timescale for delivering an exit plan to maintain continuity of service.

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form and an exit plan in line with the Call-Off Contract terms which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to deliver consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Partnerships/Alliances

There are no partnerships or alliances involved in this service.

10 Vendor Accreditations/Awards



For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.



ISO 9001 Quality Management for Management Consultancy and IT Implementation and services to the Public Sector



ISO 27001:2013 - Provision (Delivery) of IT services including business applications development, maintenance and Data, Digital and Cloud technologies.



NelsonHall has identified Capgemini as a Leader in its 2022 NEAT Vendor Evaluation for Learning Services due to its ability to meet future client requirements as well as its capability to deliver immediate learning benefits to them.



Capgemini is the first amongst consultancy and technology firms to be recognized six times in a row for its thought leadership reports.



2023 Ecovadis Platinum Rating: We maintained a platinum rating, recognising us as a responsible and sustainable business in the top 1% of companies assessed.



Better Society Awards: Our collaboration with Code Your Future to offer digital skills training won a Better Society Award in 2022. The awards celebrate efforts by commercial organisations to create a better society.



Inclusive Top 50 UK Employers List: We achieved second place in the Inclusive Top 50 UK Employers List 2022/23 – a list that assesses companies for best practice on diversity, equality and inclusion



UK Best Workplaces for Women: We were listed as a Best Workplace for Women by Great Place to Work®. This listing is based on responses from our team to an anonymous survey about their employee experience.



UK Best Workplaces for Wellbeing: We are listed by Great Place to Work® as a Best Workplace for Wellbeing



Great Place to Work: We were certified as a Great Place to Work® in 2023, reflecting our employees' experience of working at Capgemini in the UK.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.



12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

15 Further Information

In addition to Cybersecurity awareness, behaviour and culture services, Capgemini can provide a range of cybersecurity services such as – cybersecurity maturity, strategy and transformation, security management, governance risk and compliance, architecture design & implementation, identity and access management, cyber analytics & protective monitoring, digital forensics and testing.

Capgemini has over 500 security professionals based in the UK whose expertise can be leveraged to provide Buyer's with cybersecurity services.

For more information about this or any of Capgemini's G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2026 Capgemini. All rights reserved.