


# Cyber Security Culture Assessment

A QinetiQ Cyber Security Service

## Key Benefits

### Key Benefits

- Ability to understand the security behaviors and security culture of the wider organisation.
- Identifies areas where security culture and security practices can be improved.
- Measuring and understanding security culture provides a critical insight into understanding how prepared an organisation is to prevent security incidents and to respond to them when they occur.

Cyber-enabled technology supports an enormous variety of business activities, resulting in a complex socio-technical system that depends as much on the behaviour of individuals as it does technological security controls. Measuring and understanding security culture provides a critical insight in understanding how prepared an organisation is to prevent security incidents and to respond to them when they occur. Technology can only do so much in protecting a business against a breach when attackers are exploiting human behaviour so that attacks are more likely to be successful and have a bigger impact.

The 2025 Cyber Security Breaches Survey from the Department for Science Innovation and Technology (DSIT) highlights a changing cyber landscape with ever-evolving threats to be managed.

According to the survey, phishing attacks remain the most prevalent form of attack experienced by organisations. They are also considered to be the most disruptive because of the volume and frequency by which they occur, and the need for increased staff training as a result of them.

Artificial Intelligence (AI) impersonation has added further challenge and complexity to this problem.

A lack of understanding about how to mitigate against the unintended consequences of employee behavior is leaving UK businesses vulnerable to not only the most common type of security breaches, but also the most disruptive and expensive. Security breaches are now seen by many organisations as inevitable, and where the impact must be prepared for and managed. Having a strong security culture is crucial. It is at its most effective when everyone understands the importance of effective security and how the wrong security behaviour can create vulnerabilities and impact the organisation's ability to respond.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

Certified Service
Cyber Security Consultancy - Risk Assessment
Certified Service
Cyber Security Consultancy - Audit & Review
CREST
CHECK
IT Health Check Service
THE CYBER SCHEME

# The QinetiQ Approach

Organisational culture and employee attitudes towards security are critical to providing enhanced security at an enterprise level. We define Security Culture as:

*'The assumptions, values, attitudes and beliefs held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not have an explicit, known, link to that impact'.*

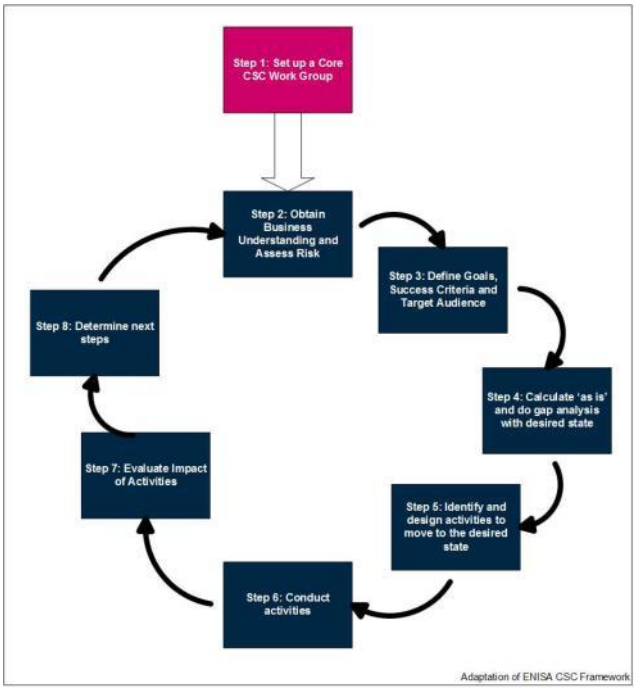
More simply, we think of it as understanding whether everyone in the organisation:

- Knows what to do;

- Can do what is being asked of them; and

- Is willing to behave as desired when faced with competing pressures.

When thinking about culture change we encourage our clients to consider the model proposed by ENISA[3]:




Cyber Security Culture in Organisations. ISBN 978-92-9204-245-5 DOI 10.2824/10543)

The Cyber Security Culture assessment service begins with a standardised 90-item questionnaire that all employees are encouraged to complete.

The questionnaire allows organisations to further their understanding of how their employees behave with regards to security. Specifically, **our assessment allows you to understand where behaviours within your workforce are the same or different.** We recognise that not all employees are the same and that different teams will behave in different ways. We also understand that this difference can both help provide effective security and at other times make the organisation more vulnerable to risks.

The Security Culture Assessment has been developed over many years. It is **based on scientific evidence of the factors that lead to effective security cultures within organisations across the Critical National Infrastructure**. The questionnaire outputs are based around our seven factors of security culture:

- Security as a core value.

- Leadership and line management.

- Security awareness.

- Individual employee behaviors.

- Physical security.

- Incident reporting.

- Perceived impact of security on the day job.

The analysis compares different parts of organisations (e.g. departments and locations) as well as organisational and demographic information (e.g. age, gender, seniority) to identify how behaviors are similar and different across the organisation. By basing internal security strategy around these issues, **employees will be motivated to remain alert to risks and unusual behaviours;** will be more engaged and productive; and businesses will be more secure as a result.

Once this initial questionnaire-based assessment is complete, it is important to understand why the current attitudes to security exist. This allows organisations to fully understand both the enablers and barriers to security culture within the organisation, and identify the steps that need to be taken to undertake a focused culture change programme that delivers behavioural change in the right areas.

Once cultural changes have been delivered and embedded, it is important to then assess their impact by repeating the initial assessment to determine why employees hold different attitudes and beliefs.

## Why QinetiQ Cyber

- Unmatched team of vetted, expert cyber consultants, architects, engineers and human performance scientists.
- Unique experience and patented intellectual property in securing the world's most complex, safety critical environments.
- Highly qualified Cyber Professionals.

**For further information please contact:**

Malvern Technology Centre St Andrews Road, Malvern Worcestershire, WR14 3PS
United Kingdom
+44 (0)1252 392000
cyberenquiries@QinetiQ.com
www.QinetiQ.com

Copyright QinetiQ Ltd 2026 | CYBER SECURITY CULTURE ASSESSMENT SERVICES


[3] ENISA (2017) Cyber Security Culture in Organisations. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations