CyberSecurity Culture (CSC)

Return to Glossary

CyberSecurity Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding Cybersecurity and how these manifest in people's behavior with information technologies. **CyberSecurity Culture (CSC)** is about making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions. Adopting the right approach to information security enables a resilient **CyberSecurity Culture (CSC)** to develop naturally from the behaviors and attitudes of employees towards information assets at work, and as part of a company's wider organizational culture, its **CyberSecurity Culture (CSC)** can be shaped, directed and transformed. However, business environments constantly change, hence organizations must actively maintain and adapt their **CyberSecurity Culture (CSC)** in response to new technologies and threats, as well as their changing goals, processes and structures. A successful **CyberSecurity Culture (CSC)** shapes the security thinking of all staff (including the security team), improving resilience against all cyber threats, especially when initiated through social engineering, while avoiding imposing burdensome security steps preventinng staff from effectively performing their key business functions.

Source: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations