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 they manifest in people's behaviour with information technologies. 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 CSC to develop naturally from the behaviours and attitudes of employees towards information assets at work,1and as part of a company's wider organisational culture, its CSC can be shaped, directed and transformed.2However, business environments constantly change, hence organisations must actively maintain and adapt their CSC in response to new technologies and threats, as well as their changing goals, processes and structures. A successful CSC shapes the security thinking of all staff (including the security team), improving resilience against all cyber threats, especially when initiated through social engineering,3while avoiding imposing burdensome security steps that prevent staff from effectively performing their key business functions.

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