Maddie Rayment

Building a Strong Cyber Security Culture in Small and Medium-Sized Enterprises (SMEs)

WHAT IS A CYBER CULTURE?

A strong cyber culture is the shared understanding of what is normal and valued in relation to cybersecurity, including expected behaviours, collaboration, trust and learning. While it differentiates based on SMEs technological needs, it should always create environments that engage with business goals.

RECENT DATA FROM 2024-25

- In 2025, findings found that SMEs believe they are “too small to be targeted” by any cyber threats. This explains the relaxation of promoting risk awareness and responses.
- It was discovered that 67% of SMEs lack fully actionable cyber security strategies which means they are more prone to risk of attacks.
- In 2024, it was found that more than 35% of SMEs experienced at least one cyber incident, yet a large share of this percentage had no security protections OR training.

BUSINESSES AND CYBER THREATS

It is important for SMEs to understand the different kinds of threats they may encounter and to respond appropriately and effectively. Here is a list of the most common risks:

- Phishing Emails: revealing credentials by clicking malicious links.
- Ransomware: malware which encrypts data and demands ransom – these attacks have risen sharply due to lacked efficient response strategies.
- Data Breaches: illicit access of confidential information collected by SMEs through their customers.
- Human Error Incidents: lack of cyber knowledge may lead to mishandling of information, for example, poor password management.

CYBER CULTURE PRINCIPLES

Every business is different, so requires different cyber security to prevent attacks. Therefore, a strong cyber culture cannot be generalised to every single business as it will not support SME needs. In response to this and to support businesses, the National Cyber Security Centre (NCSC) created six core principles to help create the strongest cyber culture in workplaces across the UK by encouraging cyber resilience.

Maddie Rayment

Cyber security as an enabler to help achieve goals

Cybersecurity should be viewed as an enabler for SMEs rather than a barrier to progress. By implementing simple, effective safeguards that protect without being complicated, businesses can achieve their goals while minimising exposure to threat.

Building safety, trust and processes to encourage openness around security

Businesses should promote early reporting of suspicious activity to prevent cyberattacks, incorporating a blame-free culture that emphasises learning which strengthens cybersecurity resilience.

Embrace change to manage threats and use opportunities to improve resilience

SMEs should adopt new technologies alongside providing cybersecurity training to ensure employees understand risks and can respond effectively to threats, strengthening resilience and informed decision making.

Organisational social norms to promote secure behaviour

SMEs should ensure their employees practice good cyber behaviour through reporting risks and completing training. This enables SMEs to identify and reduce risky habits, such as sharing confidential information.

Leaders take responsibility for impact they have on cyber security culture

Owners and managers of SMEs should lead by example through encouraging completion of cyber training, championing positive practices and ensuring cybersecurity is embedded across all staff and daily operations.

Well maintained cyber security guidelines

SMEs should maintain clear, up-to-date cybersecurity guidelines. They should be integrated into training and leaders should consistently promote them in daily operations.

CONCLUDING STATEMENTS: WHAT CAN SMEs DO TO BUILD THIS CULTURE?

To maintain a strong cybersecurity culture, SMEs should adopt these key practices:

- Providing clear cybersecurity guidance
- Encourage a blame-free culture regarding risk reporting to promote learning.
- Business leaders model and reinforce good cyber practices.
- Deliver regular training to educate and build strong understanding of cybersecurity.
- Strong password measures, such as password managers and multi-factor authentication.