



CYBER ESSENTIALS PLUS

KEY CONTROLS



An Exploratory Study of Adapting the UK Cyber Essentials Plus Scheme for Irish SMEs

Introduction

Small and medium-sized enterprises (SMEs) are essential to the Irish economy, but they are increasingly targeted by cyberattacks such as phishing, ransomware, and data breaches. Many SMEs lack the resources and expertise to protect themselves, while existing cybersecurity frameworks are often too complex and expensive. Therefore, this study explores how the UK Cyber Essentials Plus scheme can be adapted to provide a simple and effective cybersecurity solution for Irish SMEs.

Research Objectives

- ✓ To identify and analyse the key barriers to cybersecurity adoption among Irish SMEs
- ✓ To evaluate the effectiveness and suitability of Cyber Essentials Plus for Irish SMEs
- ✓ To examine how Cyber Essentials Plus can align with Ireland's Cyber Fundamentals (CyFun) framework and EU cybersecurity regulations



Top Research Question

How can the UK Cyber Essentials Plus scheme be adapted to meet the cybersecurity needs of Irish SMEs?

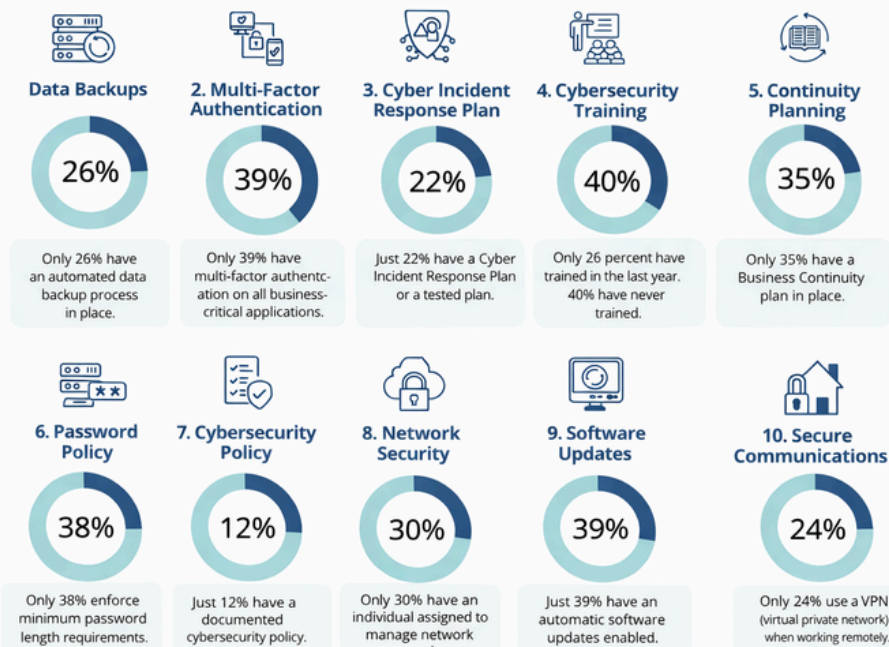
Preliminary Insights and Analysis

Common Cyber Threats to SMEs



Top Cyber Resilience Weaknesses for Irish SMEs

Analysis identifies 10 key areas where Irish SMEs consistently underperform. These weaknesses greatly increase vulnerability to cyber incidents. Addressing even a few of these gaps can significantly improve an SME's resilience.



Key Findings from Literature Review

- Research shows that SMEs are highly vulnerable to cyberattacks due to limited resources, skills, and cybersecurity systems. Common threats include phishing, ransomware, and data breaches.
- Existing frameworks such as ISO 27001 and NIS2 are often too complex and costly for SMEs to implement effectively.
- The UK Cyber Essentials Plus (CE+) scheme provides a simpler and more affordable approach by focusing on five key controls: firewalls, secure configuration, access control, malware protection, and software updates. It has been shown to improve basic cybersecurity protection in organisations.

Method

Research Design

Mixed-method approach combining quantitative and qualitative data.

Participants

- ✓ 50+ Irish SMEs across different sectors.
- ✓ Cybersecurity professionals

Conclusion

- ✓ Irish SMEs face high cyber risks and struggle with complex, costly frameworks.
- ✓ Cyber Essentials Plus could improve SME cybersecurity if adapted to Ireland and supported by government.

Key Policy Insight

Cyber Essentials Plus is already proven in the UK as a government-backed cybersecurity standard for suppliers, suggesting strong potential for adoption in Ireland's public procurement system.

Cybersecurity Challenges	Proposed Solutions
High Cyber Risk	Cyber Essentials Plus (CE+) Framework
Lack of Technical Skills	Simple Cybersecurity Controls & Guidance
High Cost of Implementation	Affordable & Scalable Model for SMEs