FRANKTON

Security Industry Trends

IN-HOUSE CYBERSECURITY CONTINUES TO GROW ACROSS THE UK

January 2026 | UK Security Industry Update

www.franktongroup.com

Introduction

As cyber threats continue to rise in frequency and sophistication, cybersecurity has become a critical priority for UK organisations across all sectors. From data protection and business continuity to regulatory compliance and reputational risk, companies are reassessing how they manage digital security in an increasingly complex threat landscape.

Against this backdrop, a growing number of UK businesses are rethinking their reliance on outsourced cybersecurity services and are instead choosing to build stronger internal capabilities.

In-House Cybersecurity on the Rise

UK mid-market organisations are increasingly bringing cybersecurity operations in-house, marking a significant shift in how security services are delivered and managed. According to a January industry report, approximately 65% of UK companies now operate their own internal cybersecurity teams, rather than relying primarily on external service providers.

This change reflects a broader move toward tighter governance, improved accountability and greater resilience against cyber risk.

FRANKTON

January
2026

Why Businesses Are Moving Cybersecurity In-House

Several key factors are driving this shift across the UK business landscape:

- Trust and control: Organisations are seeking greater transparency and direct oversight of their cyber risk management, particularly where sensitive data and critical systems are involved.
- Rising cyber threats: The increase in ransomware attacks, data breaches and supply-chain vulnerabilities has pushed cybersecurity higher on board-level agendas.
- Faster response times: Internal teams enable quicker decision-making and incident response without dependency on third-party escalation processes.

Impact on the Security Services Sector

For the UK security industry, this trend signals a change in demand rather than a decline in opportunity. While some organisations are reducing their dependence on fully outsourced cybersecurity services, demand is increasing for:

- Specialist consultancy and advisory services
- Cybersecurity training and workforce development
- Hybrid security models combining internal teams with external expertise
- Advanced security technologies, monitoring tools and incident response support

Security providers are increasingly expected to support and enhance in-house teams, rather than replace them.

Skills Shortage Remains a Key Challenge

Despite the move toward internal cybersecurity teams, the UK continues to face a shortage of skilled cyber professionals. Recruiting, training and retaining qualified talent remains a challenge, particularly for mid-sized organisations competing with larger enterprises and government bodies.

This ongoing skills gap presents both risk and opportunity for security providers capable of delivering accredited training, talent pipelines and scalable cyber solutions.

Disclaimer

This article is intended for general information purposes only and does not constitute professional cybersecurity, legal or regulatory advice. The information contained herein is based on industry reports, publicly available sources and current market observations as of January 2026. While reasonable efforts have been made to ensure accuracy, security threats, technologies and regulations continue to evolve. Organizations should seek independent professional advice before making decisions relating to cybersecurity strategy, risk management or compliance.

FRANKTON

🌐 www.franktongroup.com

☎ 08081753305 / 01276786000