Cyber Security Scotland Innovation Roadmap

Opportunities, Challenges and Global Ambition

Executive Summary

Scotland's Cyber Resilient Scotland 2025–2030 Strategic Framework, together with its Action Plan and Market Development initiatives, serves as the nation's Cyber Security Innovation Roadmap.

It positions Scotland as an emerging European leader by integrating cyber resilience with economic growth. The sector has expanded rapidly, now comprising over 400 specialist firms — nearly three times the number in 2018 — with many being recent startups.

The roadmap emphasises innovation in AI-driven and IoT security, talent development targeting a 30% increase in professionals, establishment of a Cyber Innovation Hub, and international expansion through trade missions and global branding.

By 2030, it aims to boost Scotland's global market share and establish the country as a hub for ethical, innovative cyber solutions.

Scotland - European Leader in Cyber Security

Scotland is positioning itself as a European leader in cyber security through a coordinated national strategy that integrates resilience-building with innovation-driven economic growth.

The Cyber Resilient Scotland 2025–2030 Strategic Framework, published in November 2025, together with its Action Plan and supporting industry development efforts, serves as the core “Innovation Roadmap.”

This framework leverages Scotland’s academic strengths, growing startup ecosystem, and government–industry–academia partnerships to address escalating cyber threats while capturing global market opportunities.

Market Overview and Growth Trends

Scotland’s cyber security sector has experienced significant expansion in recent years.

There are now over 400 specialist cyber security goods and services businesses operating in Scotland, nearly three times as many as in 2018, with almost half being startups less than seven years old.

Within the broader UK context, the cyber security sector generated £13.2 billion in revenue in the year covered by the 2025 DSIT analysis, representing a 12% year-on-year increase, and employed approximately 67,300 people.

Scotland accounts for around 6% of UK-registered cyber security firms, with notable clusters in Glasgow and Edinburgh. Globally, cyber security spending is projected to reach between $454 billion and $522 billion in 2026, with forecasts indicating potential growth toward $1 trillion annually by 2031, driven primarily by AI-enabled threats, IoT expansion, supply-chain risks, and regulatory pressures.

Vision and Strategic Framework

The refreshed Strategic Framework sets a clear vision: “Scotland thrives by being a

digitally secure and resilient nation."

It outlines four main outcomes focused on people, businesses and organisations, digital public services, and effective national incident response, while also emphasising a seventh outcome dedicated to a flourishing cyber security industry, research community, and skilled workforce.

Complementary industry initiatives, including elements of a Market Development Plan, provide operational detail through targets such as increasing Scotland's global cyber market share, establishing leadership in AI-driven and IoT security innovation, growing the number of cyber security professionals by 30%, achieving high levels of Cyber Essentials adoption, and forging major international partnerships.

Key Innovation Initiatives

Core innovation initiatives within the roadmap include annual funding allocations through Scottish Enterprise to support research in AI, IoT, and quantum technologies.

Plans also encompass the establishment of a Cyber Innovation Hub in Edinburgh to foster collaboration among startups, universities, and larger firms, alongside a Cyber Accelerator Programme designed to support new startups each year.

Talent development features prominently, with proposals for a national apprenticeship scheme targeting 1,000 places annually by 2028 and expanded training programmes delivered through bodies such as ScotlandIS.

Internationalisation efforts include targeted trade missions and a global "Cyber Scotland" branding campaign to boost exports and attract inward investment.

SWOT Analysis

A SWOT analysis of Scotland's cyber security position reveals clear strengths alongside areas for improvement. Strengths include the rapid growth of the sector, a world-class academic pipeline featuring programmes such as ethical hacking degrees and research centres, and a collaborative ecosystem supported by the Scottish Cyber Coordination Centre and industry bodies.

Weaknesses centre on skills shortages, particularly at mid-to-senior levels, fragmented

awareness among some business leaders, and reliance on legacy systems in parts of the public and SME sectors.

Opportunities lie in export growth for AI and IoT security solutions, supply-chain resilience demands, and intersections with green technology and digital twins. Threats include intensifying AI-powered attacks, talent competition from larger hubs such as London, and potential funding or regulatory constraints.

Opportunities and Challenges

High-growth opportunities for Scotland include positioning the country as a testbed for secure AI deployment, capitalising on existing expertise in critical national infrastructure protection, fintech security, and health data. Export and inward investment potential can be realised through focused international missions and branding.

The talent pipeline can be strengthened via scaled apprenticeships and mid-career conversion programmes in emerging areas such as AI security. Persistent challenges involve closing the skills gap, ensuring broad Cyber Essentials adoption beyond larger organisations, and effectively measuring the return on innovation investments.

Recommendations

To maximise the roadmap's impact, several recommendations stand out. Implementation of the Cyber Innovation Hub and Accelerator programmes should be accelerated with full funding in the coming years.

Skills development requires priority attention through expanded apprenticeships and targeted conversion initiatives. Internationalisation efforts would benefit from consistent annual trade missions supported by export grants.

Robust annual sector benchmarking, aligned with UK-wide analyses, would help track progress in firms, revenue, exports, and employment. Finally, deeper public–private synergies, including expanded support for SMEs and managed service providers, would enhance overall resilience and growth.

Conclusion and Outlook

Scotland's Cyber Security Innovation Roadmap is both ambitious and pragmatic.

Successful execution by 2030 could establish the sector as a substantial export engine, generate thousands of high-value jobs, and cement Scotland's reputation as Europe's preferred hub for ethical and innovative cyber solutions.

The combination of the 2025–2030 Strategic Framework and associated action and market development plans offers a clear, actionable path forward. Sustained collaboration across sectors, consistent public investment, and agile adaptation to emerging threats will be essential to realising the vision of a digitally secure, prosperous, and globally competitive cyber nation in Scotland.