



THE
**CYBER
RESILIENCE
CENTRE**
NETWORK

CYBER RESILIENCE CENTRE NETWORK

STRATEGY 2025-2027



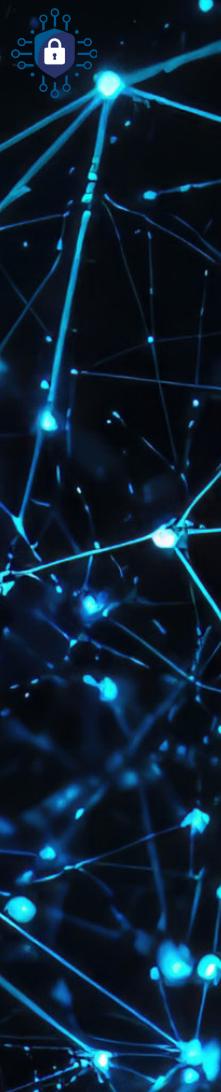


TABLE OF CONTENTS

Mission	3
Vision	5
Strategic Objectives	6

* This Strategy should be read in conjunction with the
CRC Network Operating Model.



CRC NETWORK MISSION

The Cyber Resilience Centre Network is a strategic collaboration between the police, government, private sector and academia to help strengthen cyber resilience across the sole trader, micro, small and medium-sized enterprises and third sector communities, protect the UK economy and support growth. The CRC Network is a key part of HM Government's National Cyber Strategy and the National Policing Strategy for Fraud, Economic and Cyber Crime.

Small and medium-sized organisations (SMOs) accounted for 99% of the UK business population at the start of 2024, with 99% being small businesses with fewer than 50 employees¹. Federation of Small Businesses research suggests that 77% of smaller businesses within the UK are part of supply chains². Smaller organisations typically lack in-house expertise and may never have benefited from cyber resilience advice, due to a lack of awareness of cyber threats, cost, or not knowing where to start and who to ask for help.

The CRC Network proactively identifies ways to reach Small and Medium Sized Organisations (SMOs) to provide cyber security guidance, raising awareness and encouraging behaviour change to drive cyber resilience. The CRC Network promotes and aligns with services, products and guidance from the National Cyber Security Centre (NCSC). The network is "Police-Led, Business-Focused", capitalising on the police brand as a trusted source of crime prevention guidance and support.

The CRC Network provides long-term support, through a customer journey model, involving regular, engaging bitesize cyber security guidance to members, tailored to specific regions or sectors. The journey aims to develop understanding over time.

Cyber PATH provides SMOs with fully funded cyber security services such as staff training, guidance on security policy and testing services to improve their risk awareness and cyber resilience. The CRC Network works with some of the country's top student talent, with the students delivering these services. The CRCs encourage the onward referral of members to Cyber Essentials (CE) partners and CE certification. Cyber PATH is a unique programme for workplace ready talent, aiming to address the skills crisis in industry and public sector.

The **National Ambassador Programme** provides the UK's largest organisations with an opportunity to work in collaboration with policing, to promote cyber resilience to their SMO supply chains, client base and wider SMO community.

¹ UK Small Business Statistics, Federation of Small Businesses

² Chain Reaction: Improving the supply chain experience for smaller businesses, Federation of Small Businesses Report 2018



THE CRC NETWORK SUPPORTS HM GOVERNMENT'S NATIONAL CYBER STRATEGY 2022

1

PILLAR ONE:

STRENGTHENING THE UK CYBER ECOSYSTEM:

Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber

Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber security profession that inspires and equips future talent

Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy

The CRC Network recognises that it cannot operate alone. Regional CRCs are a key part of their local Cyber ecosystem, engaging with the UK Cyber Clusters, local Chambers of Commerce, business and innovation groups and community volunteers to promote SMO cyber resilience.

2

PILLAR TWO:

CYBER RESILIENCE:

Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

Prevent and resist cyber-attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens

Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks

The overarching goal of the CRC Network, from which all activity flows, is for SMOs to **understand** cyber threats and **change their behaviour** to improve cyber resilience, making the UK a safer place.



CRC NETWORK VISION

The vision for the CRC Network is:

- To be the trusted source of cyber resilience guidance for SMOs, thereby making the UK a safer place to do business online
- To help members understand their cyber risks and improve their cyber security
- To help reduce the UK cyber skills shortage through Cyber PATH student development

CRC NETWORK STRATEGIC OBJECTIVES FY 25/26 – FY 26/27

- 1** Increase membership of priority sector - Managed Service Providers for SMOs
- 2** Increase membership of priority sector - SMOs holding large personal data sets
- 3** Supporting existing CRC members
- 4** Close alignment with National, Regional and Local Cyber Protect Teams
- 5** Integration with Cross-Government SMO cyber resilience projects and initiatives
- 6** Growing membership at scale, including through National Ambassador/large organisation campaigns across SMO customers and supply chains
- 7** Promotion of Cyber Essentials/Cyber Essentials+
- 8** Iterative improvement and innovation



ACHIEVING OUR CRC NETWORK STRATEGIC OBJECTIVES - RATIONALE AND PRINCIPLES

PRIORITY SECTORS - MANAGED SERVICES PROVIDERS FOR SMOS AND SMOS HOLDING LARGE DATA SETS.

While citizens and the wider economy are a clear priority for government in improving resilience, the Home Office, NCSC and DSIT have identified two key areas where significant widespread harm needs to be tackled.

The first is tackling the threat from infiltration of supply chains, particularly where there are digital connections allowing companies direct access into the systems of other organisations.

The second is tackling the stolen data ecosystem; protecting individuals from the downstream cybercrime and fraud attacks enabled by the exfiltration of data from cyber breaches against organisations. This is a particular concern where organisations hold data on vulnerable citizens.

SUPPORTING EXISTING CRC MEMBERS

We will improve our understanding of the impact that CRC membership and Cyber PATH services has on SMO awareness and behaviour; focusing KPIs and metrics on how engaged our membership is and what actions they took.

CLOSER ALIGNMENT WITH NATIONAL, REGIONAL AND LOCAL CYBER PROTECT TEAMS

As a key part of the wider law enforcement Team Cyber UK network, CRC Network activity will align with the National Policing Strategy for Fraud, Economic and Cyber Crime 2023–2028. Close working relationships with every part of the system; including Report Fraud, regional and force cybercrime teams, PCA and NCCU are vital to deliver as a collective; improving cyber resilience and reducing repeat victimisation.



INTEGRATION WITH CROSS-GOVERNMENT SMO CYBER RESILIENCE PROJECTS AND INITIATIVES

The CRC Network is increasingly seen as a delivery mechanism for HM Government departments to reach SMOs in every part of England and Wales, at a very local level.

As a key threat area, there are numerous different Government departments and agencies who have some involvement in cybercrime and cyber security. This poses a risk of duplication. The outcomes can include an inefficient use of limited resources, unmet demand and confused messaging to SMOs.

CRC Network activity must be situated within the wider context of cross-government objectives, with an aligned communication strategy.

GROWING MEMBERSHIP AT SCALE, INCLUDING THROUGH NATIONAL AMBASSADOR/LARGE ORGANISATION CAMPAIGNS ACROSS SMO CUSTOMERS AND SUPPLY CHAINS

The CRC Network has limited staff and resources, and a potential target audience of over 5 million SMOs. The challenge is significant. The network must adopt a delivery model that is as efficient as possible; narrowing the target audience to focus on those most at risk, or where the impact of a cyber-attack would be most significant, and amplifying the message through strategic relationships and tailored marketing activity, rather than one-to-one engagement.

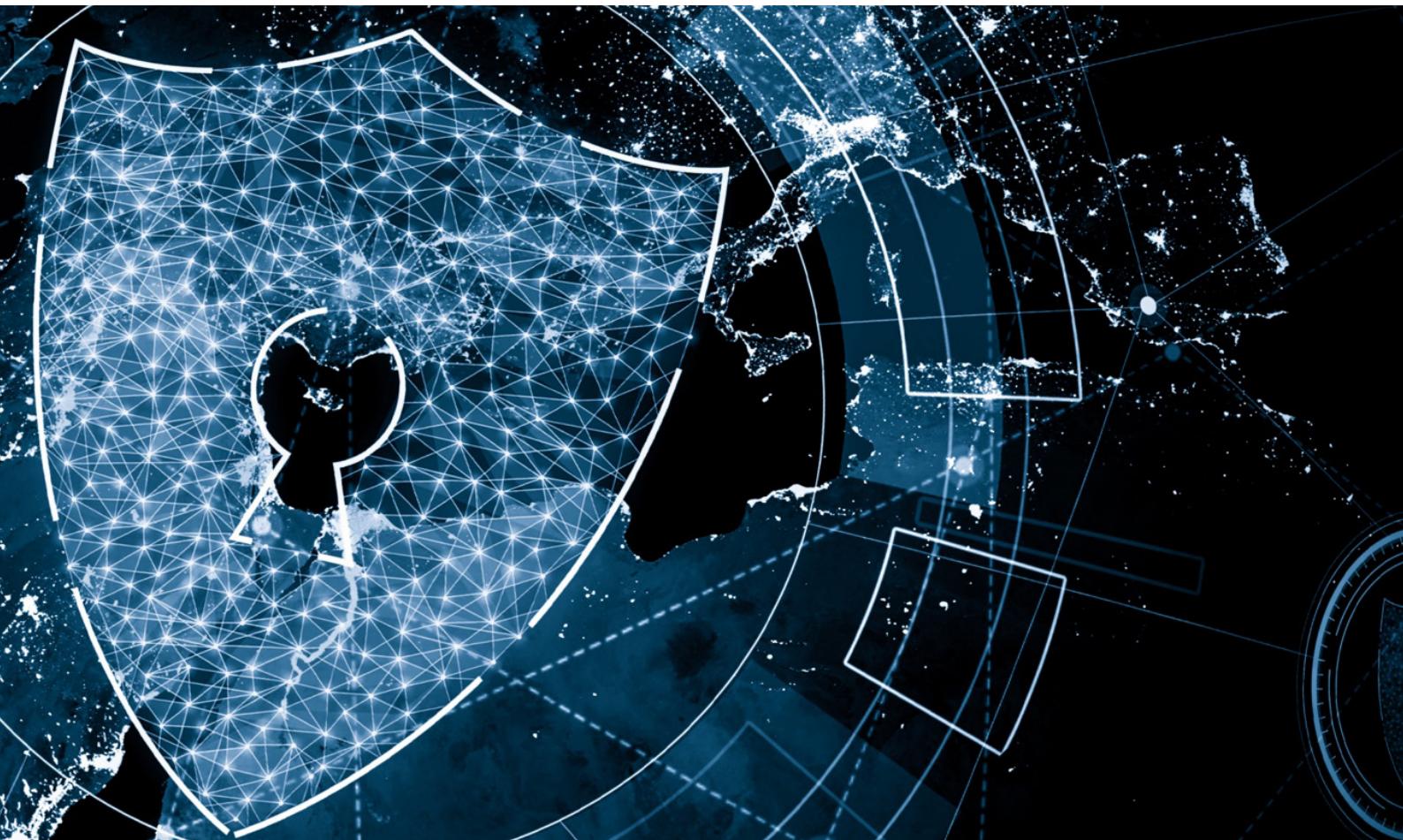
PROMOTION OF CYBER ESSENTIALS/CYBER ESSENTIALS+

Cyber Essentials represents the HM Government's minimum baseline standard for cyber security for organisations of all sizes in the UK. The annually renewable certification scheme is aligned to five technical controls designed to prevent the most common internet-based cyber security threats. Cyber Essentials certification demonstrates that an organisation is protecting itself by implementing the most important cyber security controls. Therefore, a key metric for the impact of CRC guidance and support, and demonstration of behavioural change, is for CRC members to go on to become Cyber Essentials certified.



ITERATIVE IMPROVEMENT AND INNOVATION

The network will be agile and innovative, able to test out new ideas and approaches to achieve the strategic objectives. Initiatives will be tested across multiple centres to draw on an evidence base as to what works and why. The network will proactively seek different ideas and perspectives from all staff, volunteers and local and national partners in industry and academia.





THE **CYBER RESILIENCE CENTRE** NETWORK