City of London Corporation Committee Report

Committee(s): Economic & Cyber Crime Committee	**Dated:** 23/02/2026
Subject: Cyber Resilience Centre (CRC) Network Update	**Public report:** For Information
This proposal: Updates member on the closure of regional CRCs as private businesses and future direction	Supports the CoLP Policing Plan
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£0
What is the source of Funding?	N//A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Deputy Commissioner Nik Adams
Report author:	Detective Chief Supt Andrew Gould

Summary

This report updates members on the closure of regional Cyber Resilience Centres (CRC) as private businesses and transfer of assets and staff to City of London Police and the National Cyber Resilience Centre Group, owned by the Corporation. It also outlines the new CRC Network Strategy and Delivery Plan.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. 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, medium business and third sector communities, as a key part of HM Government's National Cyber Strategy and the NPCC Cybercrime Plan. A key focus for the network is to secure supply chains and to protect the UK economy.

2. Small and medium-sized enterprises (SMEs) accounted for 99.9% of the UK business population at the start of 2024, with 99.2% being small businesses with fewer than 50 employees. SMEs make up the vast majority of the UK's supply chains. 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, prohibitive costs, or not knowing where to start and who to ask for help.

3. The CRC Network proactively identifies ways to reach SMEs to provide cyber security guidance, raising awareness and encouraging behaviour change to drive cyber hygiene. 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 policing being a trusted source of crime prevention advice, in what is recognised as a cluttered and confusing market.

4. The CRC Network provides long-term guidance, through a customer journey model, involving regular, engaging bitesize cyber security advice to members, tailored to specific regions or sectors. The journey aims to develop understanding over time. The primary aim of our student services **Cyber PATH** is to provide SMEs with fully funded cyber security services, from a trusted source, to improve their risk awareness, hopefully resulting in improved cyber resilience and onward referral to Cyber Essentials (CE) partners or CE certification.

5. There were a number of challenges that made the current operating structure untenable. These included:

- Risk of non-compliance with competition, subsidy and data sharing laws and regulation.
- Barriers to full support and public engagement by the National Cyber Security Centre (NCSC).
- Home Office, alongside NCSC and Dept Science, Innovation and Technology (DSIT), ambitions to significantly build on the regional delivery model with CRCs acting as the focal point for HMG interventions, requiring greater flexibility and accountability to central government.

- Inability to deliver sufficient effective National Police chiefs Council (NPCC) leadership and governance across the CRCs as private limited companies to ensure appropriate minimum standards and assurance required for National Cyber Security Centre (NCSC) and Home Office support.

6. A decision was made that:

1. The regional CRCs would close as businesses and be fully integrated into policing;

2. CRC staff would be line managed and led nationally from CoLP but maintain local and regional delivery through the Regional Organised Crime Units.

3. Assets and privately employed staff would transfer to the National Cyber Resilience Centre Group (NCRCG), owned by the Corporation.

Current Position

7. Expert support was engaged from Pinsent Masons and RSM to advise and assist with the transfer of CRC assets and staff. Ownership of the regional CRC companies transferred to NCRCG for voluntary liquidation to be undertaken by RSM. Transition proved to be significantly more challenging and complex than envisaged with a number of local corporate governance and other issues requiring resolution prior to transfer. These have all been resolved and all assets and staff from Wales, London, South East, Eastern, East Midlands, West Midlands, North East and North West CRCs transferred before Christmas. The South West has been delayed by staffing issues which have now been resolved and transfer is imminent. All police officers and staff seconded to their CRCs have now been seconded to City of London Police. A new network operating model was developed and delivered, is now in place and working well.

8. Last year saw a substantial increase in funding for the CRC Network from the government's Integrated Security Fund. This has funded the transition and replace previous regional private sector contributions. Going forward, we have been informed by the Home Office there may a further increase to improve our current capacity and capability, help grow our messaging and help us scale. We continue to take financial contributions from our National Ambassadors via NCRCG.

9. This will be a year of transition for the CRC Network as we move from CRCs being private businesses to being wholly controlled by policing. We are committed to embedding the new operating structure, supporting national and regional stakeholders, delivering growth in membership and service delivery. Alongside this, we have agreed CRC Network priorities and objectives with the Home Office and National Cyber Security Centre, which will focus on the following:

- Managed Service Providers for SMEs

- Small & Medium Sized Enterprises holding large personal datasets
- Supporting existing CRC members
- Closer alignment with National, Regional and Local Cyber Protect teams
- Integration with cross-government projects on SME resilience
- Growing membership, primarily through National Ambassador and large organisation campaigns across their SME customers and supply chains
- Promotion of Cyber Essentials

Options

10. None.

Proposals

11. None.

Key Data

12. CRC Network membership has grown to 29,000 across England & Wales. A performance framework is under development with the Home Office and NCSC focused on key outcomes and behaviour change including Cyber Essentials uptake.

Corporate & Strategic Implications

Strategic implications

13. Supports the CoLP Policing Plan.

Financial implications

14. None.

Resource implications

15. None.

Legal implications

16. None.

Risk implications

17. None.

Equalities implications

18. None.

Climate implications

19. None.

Security implications

20. None.

Conclusion

21. The closure of regional Cyber Resilience Centres (CRC) as private businesses and transfer of assets and staff is largely complete. This is now enabling a more consistent, high quality service to be delivered. This consistency and the new operating model will enable the large scale growth of membership and support to SMEs required to support cyber resilience in SMEs at scale.

Appendices

- Appendix 1 – CRC Network Strategy 2025-27

Andrew Gould
Detective Chief Superintendent NPCC National Cybercrime Team

T: 07596 888450
E: andrew.gould@cityoflondon.gov.uk