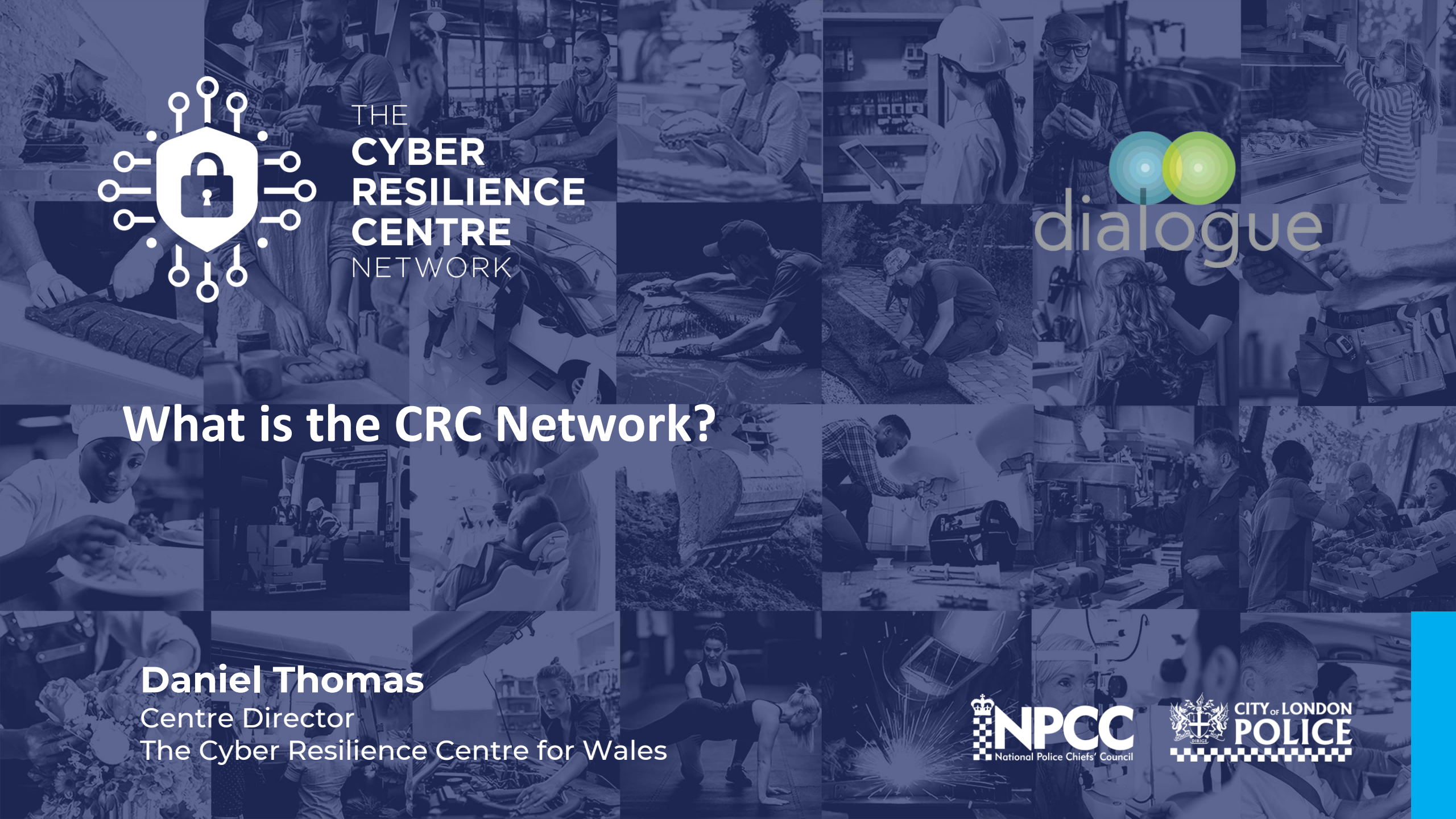


THE CYBER RESILIENCE CENTRE NETWORK

dialogue

What is the CRC Network?

Daniel Thomas
Centre Director
The Cyber Resilience Centre for Wales

NPCC National Police Chiefs' Council

CITY OF LONDON POLICE

THE CYBER RESILIENCE CENTRE NETWORK

dialogue

Police led, **business** focused cyber support organisation

Helping businesses and third-sector organisations become more secure through knowledge sharing, training, and guidance.

NPCC National Police Chiefs' Council

CITY OF LONDON POLICE

The role of the National Ambassadors

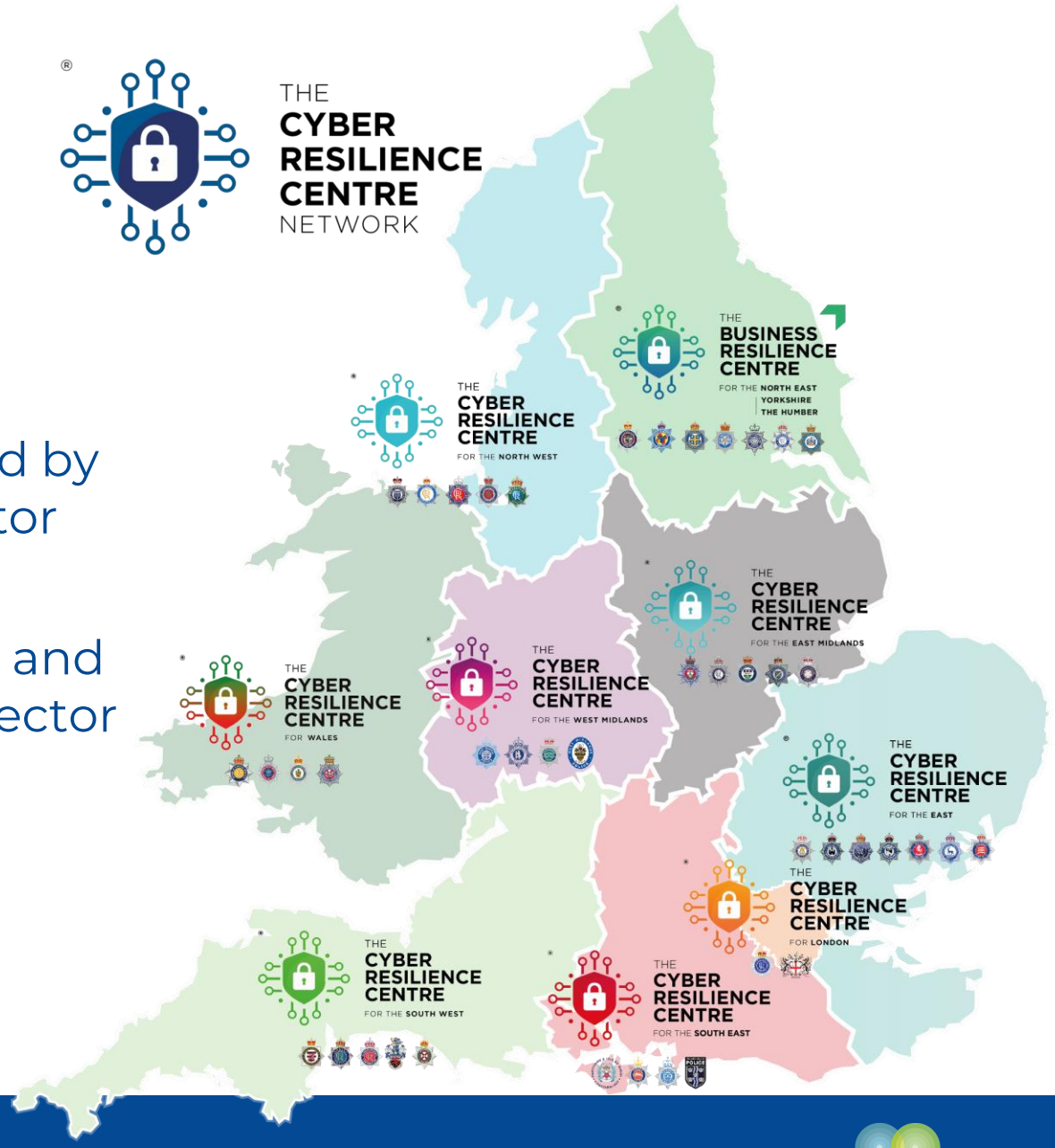
- Collaboration with senior law enforcement and government to inform on national developments on cyber resilience
- Sharing of threat intelligence to reduce the risk posed by cyber criminals
- Working closely with policing to reduce risks to supply chains, customer bases and micro, small and medium sized organisations (SMEs)
- Assisting in the development of the cyber talent pipeline

CRC Network

NATIONAL CYBER RESILIENCE CENTRE GROUP

CYBER PATH™ POLICE & ACADEMIA TALENT HORIZONS

- An organisation funded and supported by Home Office, policing and private sector partners
- Cyber support and guidance for small and medium sized businesses and third sector organisations
- A range of fully funded cyber services
- Real-life work experience for students



What your customers will receive

Real people offering real support

The teams at each CRC not only offer an initial 30-minute 1-2-1 consultation, they are also available to support members' events, such as **webinars, networking events, and community engagement.**

Daniel Thomas
Director
The Cyber Resilience Centre for Wales

The Cyber Resilience Centre for Wales

THE CYBER RESILIENCE CENTRE FOR WALES

Daniel Thomas
Director

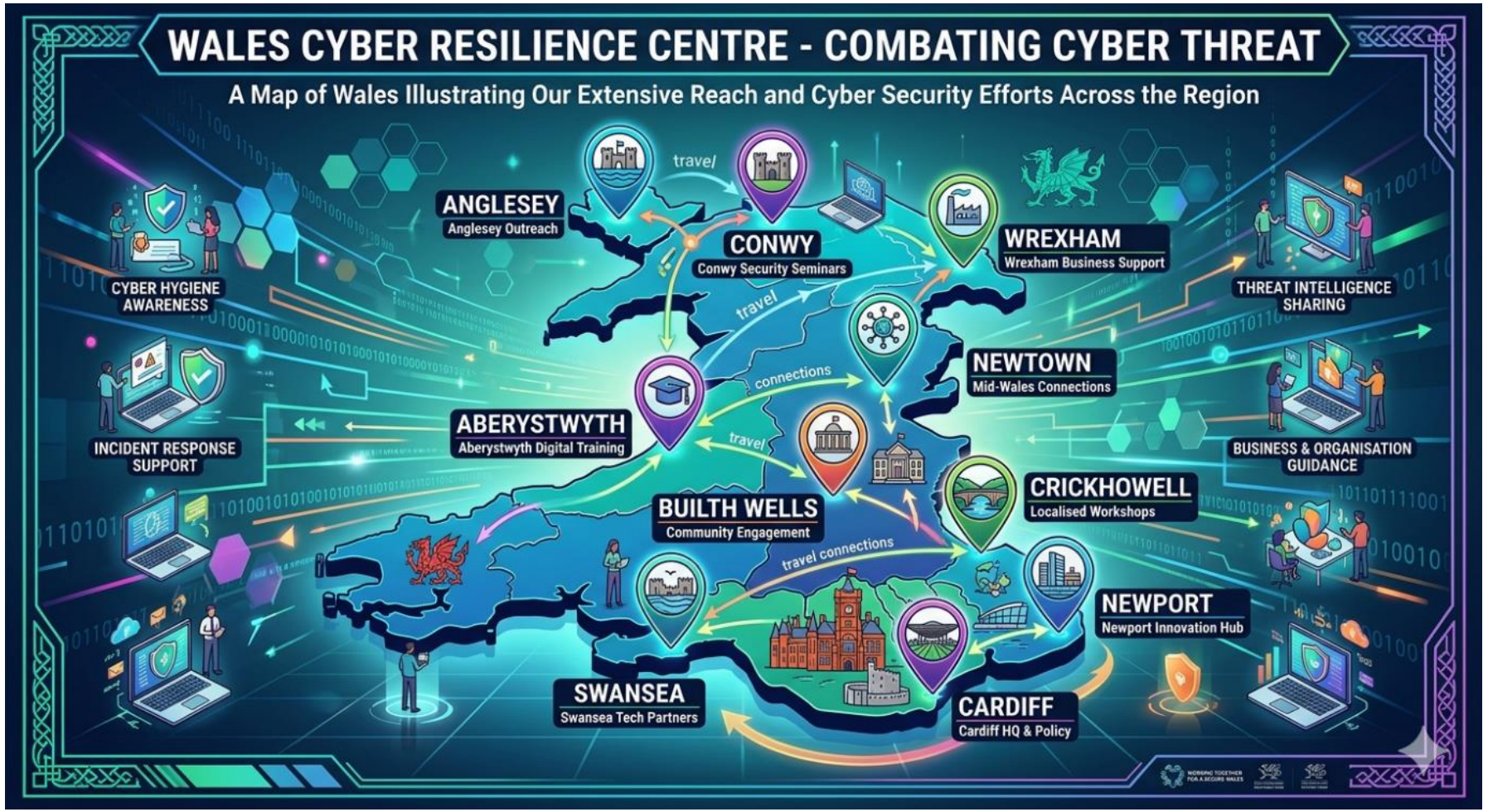
Paul Hall
Deputy Director

www.wcrcentre.co.uk

Scan the QR Code to register

We cover the whole of the country

THE CYBER RESILIENCE CENTRE FOR WALES



Collaborating with the Welsh Government

THE CYBER RESILIENCE CENTRE FOR WALES

Llywodraeth Cymru
Welsh Government

SMEs in Wales form the backbone of regional supply chains.

As these supply chains become increasingly dependent on digital systems, interconnected suppliers, and third-party platforms, they face growing exposure to cyber incidents that can disrupt operations, compromise safety, and impact the wider Welsh economy.

Collaborating with the Welsh Government

THE CYBER RESILIENCE CENTRE FOR WALES

Llywodraeth Cymru
Welsh Government

- Collaboration among Welsh Government, the Wales Cyber Resilience Centre (WCRC), and the Wales Cyber Police Protect Network
- Raise awareness, strengthen cyber resilience across the Welsh SME community.
- Help SMEs to understand supply-chain cyber risks and adopt achievable, low-cost improvements
- Delivered over six months, the project will generate measurable impact, support economic resilience and contribute to national objectives around digital skills, business continuity, and supply-chain security.

How we can help Children's Homes

THE CYBER RESILIENCE CENTRE FOR WALES

Children's homes hold some of the most sensitive data in the UK, personal histories, safeguarding information, medical details, and daily records of vulnerable young people. This makes them a prime target for cybercriminals.

The WCRC helps protect children's homes by strengthening their cyber resilience in simple, practical, and affordable ways.

How we can help Children's Homes

THE CYBER RESILIENCE CENTRE FOR WALES

Why It Matters

A cyber incident in a children's home can:

- Expose a child's location or personal history
- Disrupt care operations
- Damage trust with regulators and local authorities
- Put vulnerable young people at risk
- The WCRC helps prevent this by giving children's homes the tools, training, and support they need to stay safe.

The Cyber Resilience Centre Network

NATIONAL CYBER RESILIENCE CENTRE GROUP

THE CYBER RESILIENCE CENTRE NETWORK

CYBER PATH™ POLICE & ACADEMIA TALENT HORIZONS

- Membership is free and starts SMEs on a 16-part journey towards better cyber resilience
- Guiding them to trusted resources

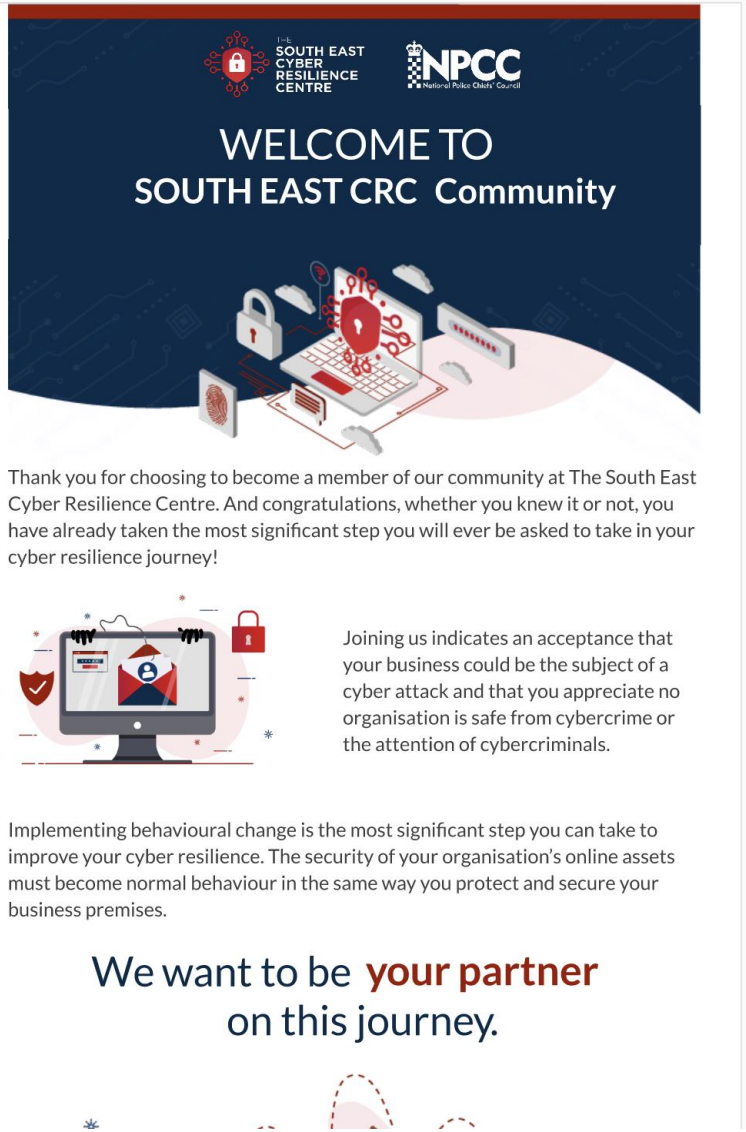
National Cyber Security Centre
a part of GCHQ

- **Encouraging them to adopt Cyber Essentials as a minimum standard**

CYBER ESSENTIALS

- **Helping them protect themselves and those in their supply chains**

CYBER ESSENTIALS PLUS



CRC membership includes:

Security Awareness Training

Ensure their team is cyber-aware, and doing the right things to protect themselves and the organisation

Signposting to free, trusted guidance

We provide details about where to go for free and highly trusted support and guidance; much of which is sector and industry-specific.

1-2-1 security discussion with a member of the CRC team to review their business's cyber resilience

Exercise in a Box

A suite of preparedness exercises based on real-world scenarios to test your organisational responses.

A Board Toolkit

Designed to support essential cyber security discussions between the board/trustees and the technical experts.

Monthly Newsletter

To keep you updated with current threats and what to look out for.

Access to a range of fully funded Cyber PATH services

Cyber PATH provides services specifically designed for SMEs and third-sector organisations.

Invitations

To webinars, drop-in surgeries, networking events and conferences.

Cyber PATH: Developing the cyber talent pipeline

CYBER PATH™
POLICE & ACADEMIA TALENT HORIZONS

Sapphire Little
Former Cyber PATH student now working full-time in cyber with Eastern CRC

- Currently working with 29 universities
- Students are provided with paid real-world workplace experience
- Students can explore cyber as a rewarding career path
- 100+ students are on, or have completed, the Cyber PATH Programme
- Until 31st March 2025, 559 days of real-world work experience had been delivered
- Many students are now working in cyber roles in policing and the private sector

Cyber PATH students provide a range of services

CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS

Security Awareness Training

Staff training for those with little or no cyber security or technical knowledge.

First Step Web Assessment

Provides you with an initial assessment of your website to highlight its most pressing vulnerabilities.

Internal Vulnerability Assessment

Scan and review your internal networks and systems looking for vulnerabilities.

External Vulnerability Assessment

Focuses on identifying weaknesses in the way your organisation connects to the internet.

Web Application Assessment

This service assesses your website and web services for weaknesses.

Microsoft 365 Service

Reviews your Microsoft 365 configuration to identify any flaws and weaknesses in your organisation's set up.

Internet Discovery Service

Comprehensive review of publicly available information about any potential or existing employee.

Cyber Business Continuity Review

A thorough review of your business continuity plan and overall resilience to cyber attacks.

Cyber Security Policy Review

An in-depth review of how your current cyber security policy is written and implemented.

THE CYBER RESILIENCE CENTRE NETWORK

dialogue

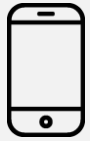
Why is SME cyber resilience important to enterprise organisations?

NPCC National Police Chiefs' Council

NATIONAL CYBER RESILIENCE CENTRE GROUP

Why focus on reaching the SME community?

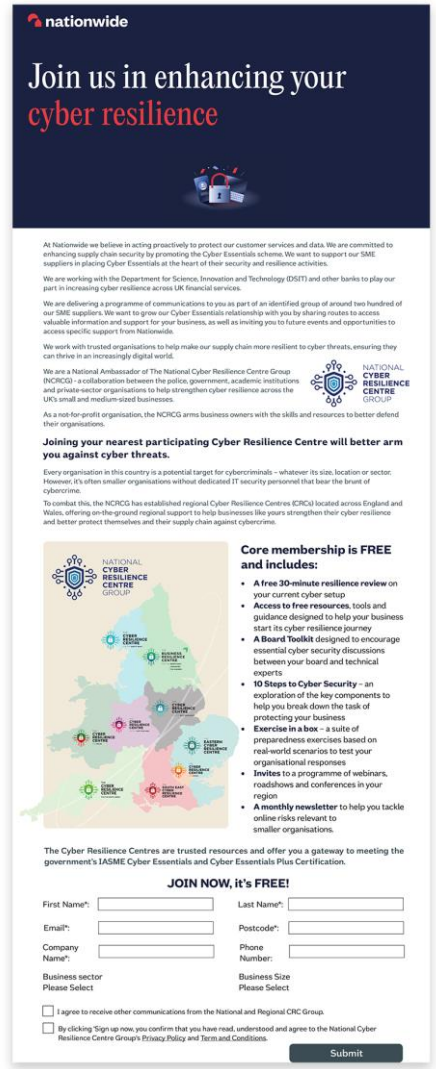
Key Facts

50%		Online Fraud and Cybercrime equates for 50% of all recorded crime in England and Wales	**75%**		65% of cyber crime victims ascribe phishing as the most disruptive type of breach
41%		41% of health or care organisations fell victim to cybercrime in last 12 months	**£9.5K**		A successful cyber security breach could result in costs of around £9528 for micro/small businesses
75%		The most common type of cyberattack was phishing attempts (75%)	**45m**		45m reported scams as of August 2025

Stats from the UK Cyber Breaches Survey 2025

Why focus on reaching the SME community?

- Most enterprise organisations have multiple SMEs in their supply chain
- Businesses are only as strong as their weakest link
- SMEs are potentially your weakest link because:
  - they don't have in-house resources and expertise
  - they are time poor
  - they don't believe they are at risk
  - they don't know what they don't know!
- Nationwide is running supply chain campaigns



nationwide

Join us in enhancing your cyber resilience

At Nationwide we believe in acting proactively to protect our customer services and data. We are committed to enhancing supply chain security by promoting the Cyber Essentials scheme. We want to support our SME suppliers in placing Cyber Essentials at the heart of their security and resilience activities.

We are working with the Department for Science, Innovation and Technology (DSIT) and other banks to play our part in increasing cyber resilience across UK financial services.

We are delivering a programme of communications to you as part of an identified group of around two hundred of our SME suppliers. We want to grow our Cyber Essentials relationship with you by sharing routes to access valuable information and support for your business, as well as inviting you to future events and opportunities to access specific support from Nationwide.

We work with trusted organisations to help make our supply chain more resilient to cyber threats, ensuring they can thrive in an increasingly digital world.

We are a National Ambassador of The National Cyber Resilience Centre Group (NCRCG) - a collaboration between the police, government, academic institutions and private-sector organisations to help strengthen cyber resilience across the UK's small and medium-sized businesses.

NATIONAL CYBER RESILIENCE CENTRE GROUP

As a not-for-profit organisation, the NCRCG arms business owners with the skills and resources to better defend their organisations.

Joining your nearest participating Cyber Resilience Centre will better arm you against cyber threats.

Every organisation in this country is a potential target for cybercriminals – whatever its size, location or sector. However, it's often smaller organisations without dedicated IT security personnel that bear the brunt of cybercrime.

To combat this, the NCRCG has established regional Cyber Resilience Centres (CRCs) located across England and Wales, offering on-the-ground regional support to help businesses like yours strengthen their cyber resilience and better protect themselves and their supply chain against cybercrime.

NATIONAL CYBER RESILIENCE CENTRE GROUP

Core membership is FREE and includes:

- **A free 30-minute resilience review** on your current cyber setup
- **Access to free resources**, tools and guidance designed to help your business start its cyber resilience journey
- **A Board Toolkit** designed to encourage essential cyber security discussions between your board and technical experts
- **10 Steps to Cyber Security** – an exploration of the key components to help you break down the task of protecting your business
- **Exercise in a box** – a suite of preparedness exercises based on real-world scenarios to test your organisational responses
- **Invites** to a programme of webinars, roadshows and conferences in your region
- **A monthly newsletter** to help you tackle online risks relevant to smaller organisations.

The Cyber Resilience Centres are trusted resources and offer you a gateway to meeting the government's IASME Cyber Essentials and Cyber Essentials Plus Certification.

JOIN NOW, it's FREE!

First Name*: Last Name*:

Email*: Postcode*:

Company Name*: Phone Number:

Business sector Please Select

Business Size Please Select

I agree to receive other communications from the National and Regional CRC Group.

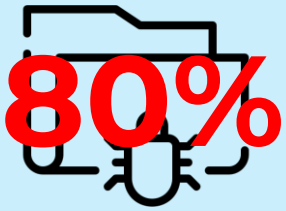
By clicking 'Sign up now, you confirm that you have read, understood and agree to the National Cyber Resilience Centre Group's Privacy Policy and Term and Conditions.

Submit

Case Study –

Manufacturing business almost had to throw in the towel

A medium-sized manufacturing company operating under a hybrid working model experienced a major cyber incident that severely impacted both its IT infrastructure and production capability.



Case Study –
Manufacturing business almost had to throw in the towel

Impact:

- Loss of critical business data
- Significant operational downtime
- Halting of production
- Financial and reputational damage

THE CYBER RESILIENCE CENTRE FOR WALES

Case Study –

Manufacturing business almost had to throw in the towel

Remedial Measures (with WCRC Support):

With guidance from the Wales Cyber Resilience Centre, the business identified several key actions to prevent a recurrence:

- Staff Cyber Awareness Training
- Anti-Malware and Endpoint Protection
- Network Segmentation
- Device Monitoring and Access Control
- Engagement with the WCRC

THE CYBER RESILIENCE CENTRE FOR WALES

THE CYBER RESILIENCE CENTRE NETWORK

dialogue

If you think your knowledge and skills could help in your local community contact;

Daniel Thomas
daniel.thomas@wcrcentre.co.uk

THE CYBER RESILIENCE CENTRE NETWORK

dialogue

Thank you for listening

Any questions?