



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



london plus



**London Communities
Emergency Partnership**



Securing charities and community groups: A Police-led initiative



Police-led, Charity & Community Group-focused cybercrime prevention



Richard Morrison-Butcher

Detective Chief Inspector

Director at The Cyber Resilience Centre for London

- NPCC Cybercrime Portfolio
- 19 years of experience in UK policing, specialising in cybercrime investigation, fraud, digital forensics, and complex case management.
- Held national coordination roles.
- Recent postgraduate of Information Security postgraduate.
- Alongside policing expertise, private sector experience from running a small business, providing a unique understanding of the challenges and opportunities facing London's business community.



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



london plus



**London Communities
Emergency Partnership**



Understanding the scale of the problem and why you are targeted





Understanding the scale of the problem

Key Facts

28%	 UK charities experiencing a cyber security breach or attack in last 12 months	£14.7bn	 Estimated cost to UK businesses from cyber attacks
57%	UK charities experience an increasing amount of phishing only attacks - the most common type of cyber incident	38%	 Ransomware attacks remain persistent amongst businesses and charities
50%	At 50%, Cybercrime & fraud is the most common crime in the UK	5.19m	 Number of cyber crimes UK businesses estimated to experience

DSIT (2026) Cyber Security Breaches Survey. DSIT (2026) Gov Cyber Resilience Pledge. Report Fraud (2026) Report Fraud Launches.



Understanding the scale of the problem

Insights

Hostile cyber activity in the UK is growing more intense, frequent and sophisticated.

(DSIT 2026)

There is a direct and active threat to our economic and national security which requires an urgent collective response.

(DSIT 2026)

- Cyber incidents are common across the charitable sector
- Phishing is the primary threat facing charities
- Cyber incidents impact finances, data, service delivery and reputation
- Smaller organisations may struggle to detect and respond
- Cyber breaches and cybercrime (including fraud) are closely linked
- Cyber risk increases as charities grow and digitise

Why charities and community groups are important



Concentration
of highly
sensitive and
exploitable
personal data

Trust makes
social
engineering
easier

Limited
budgets and
specialist
capability

Reliance on
email,
volunteers and
remote working

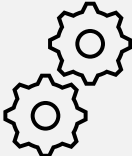
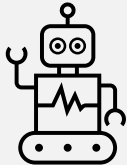
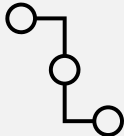
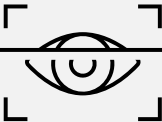
Operational
disruption
causes
disproportionate
harm

Your charity matters – so does everyone who depends on it



Scale of the vulnerability within charities

Key Fact (insights)

13%	 Report having the technical controls associated with Cyber Essentials	35%	 Insured against cyber risks
27%	 Cybersecurity processes or practices to manage the risk from Artificial Intelligence	17%	 Use Virtual Private Networks (VPN) for remote working
9%	 Review their immediate supply chain risks, dropping to 4% for wider supply chain risks	38%	 Implemented Two Factor Authentication (2FA)

DSIT (2026) Cyber Security Breaches Survey.



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



london plus



**London Communities
Emergencies Partnership**



Police-led, charity & community group- focused cyber support & the role you play in supporting your communities

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



The Cyber Resilience Centre Network



NATIONAL
CYBER
RESILIENCE
CENTRE
GROUP

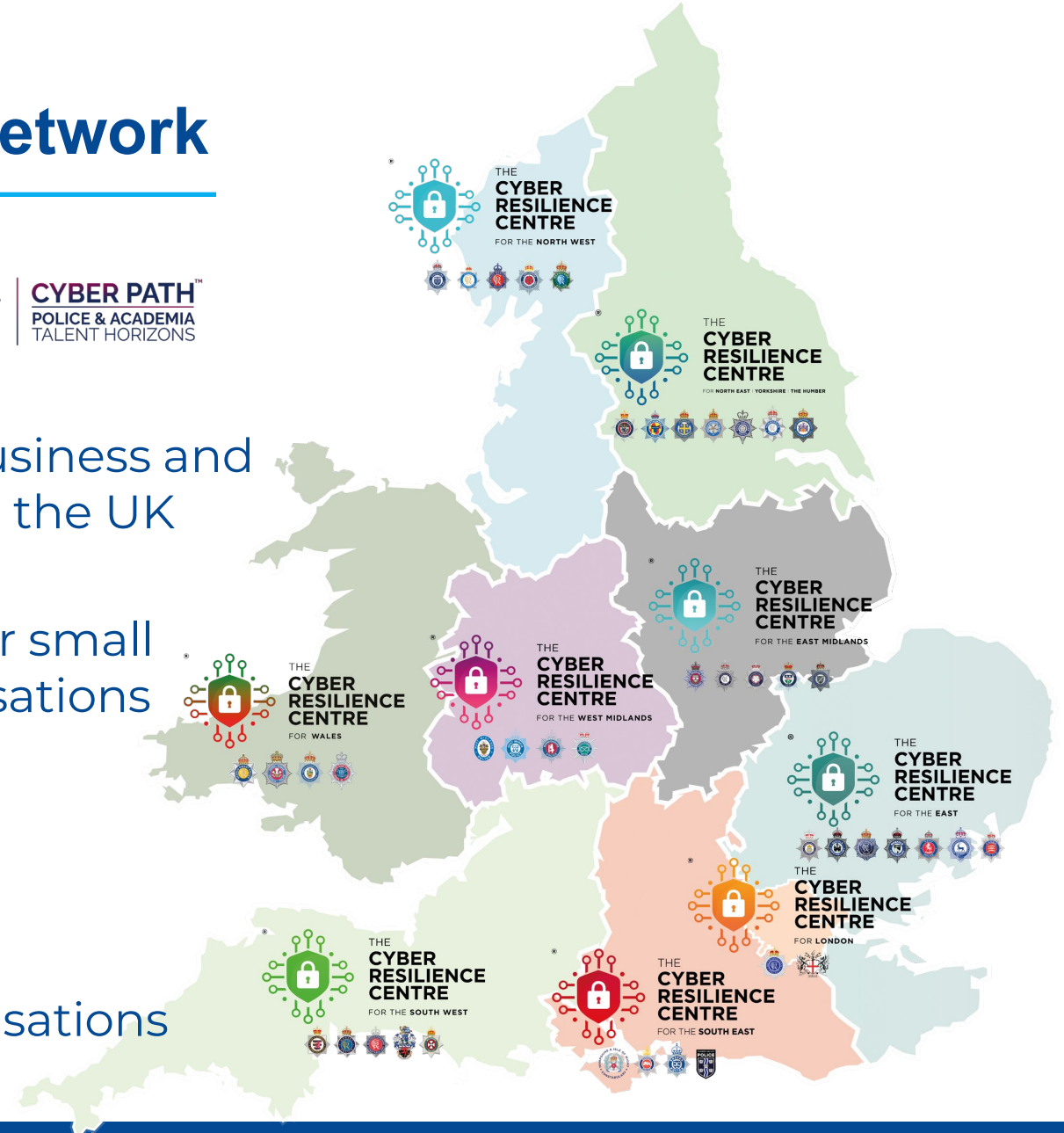


THE
CYBER
RESILIENCE
CENTRE
NETWORK



CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS

- A policing-led, government funded, business and charity-focused collaboration securing the UK economy
- Free cyber support and guidance at for small and medium sized third sector organisations
- A range of fully funded cyber services
- Real-life work experience for students
- Services available to charities, social enterprises, faith and volunteer organisations



THE
CYBER
RESILIENCE
CENTRE
FOR LONDON

Police-led, Business-focused



londonplus

London Communities
Emergencies Partnership



The Cyber Resilience Centre Network



- Membership is free and starts SMEs on a 16-part journey towards better cyber resilience
- Guiding them to trusted resources
- Encouraging them to adopt Cyber Essentials as a minimum standard
- Helping them protect themselves and those in their supply chains



THE CYBER RESILIENCE CENTRE FOR LONDON **NPCC** National Police Chiefs' Council

BUILDING BETTER CYBER SECURITY

We will only ever share with you information from trusted sources. In this email, we have added some more material from the National Cyber Security Centre (NCSC) and some other trusted providers.

These resources have been created to help business owners. You do not require any technical expertise to follow the simple advice and guidance, but it will be extremely useful in building better cyber protection for you and your business.

RESOURCES, TOOLS AND SUPPORT FOR YOUR BUSINESS.

The [National Cyber Security Centre \(NCSC\)](#) is the UK's independent authority on Cyber Security. The centre has vast technical capabilities and expertise, which they utilise to produce practical guidance for businesses and the public. They are a fantastic resource for the very latest Cyber Security guidance.

CRC membership includes



Security Awareness Training

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



1-2-1 crime prevention discussion

with a member of the CRC team to review their organisation's cyber resilience



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.

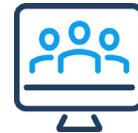


Access to a range of fully funded Cyber PATH services

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



Regional threat updates and scam alerts



Invitations

News about webinars, roadshows and business networking events



Monthly Newsletter



Trusted resources

NCSC Cyber Action Toolkit

Free

Clear, bite-sized actions

Quick to start

Complete at your pace

Builds layers of protection



<https://www.cyberactiontoolkit.service.ncsc.gov.uk>

CRC membership includes – establishing relationships

Establishing ongoing trusted relationships

Offers actionable and proportionate support; CRC fully funded services are vital to organisations with resourcing limits, and these relationships build resilience and deliver community impact, encouraging a journey towards **Cyber Essentials**.

Awareness session delivered through Charity One Westminster in partnership with Westminster City Council Resilience Officer to charities impacted by the council Ransomware attack.



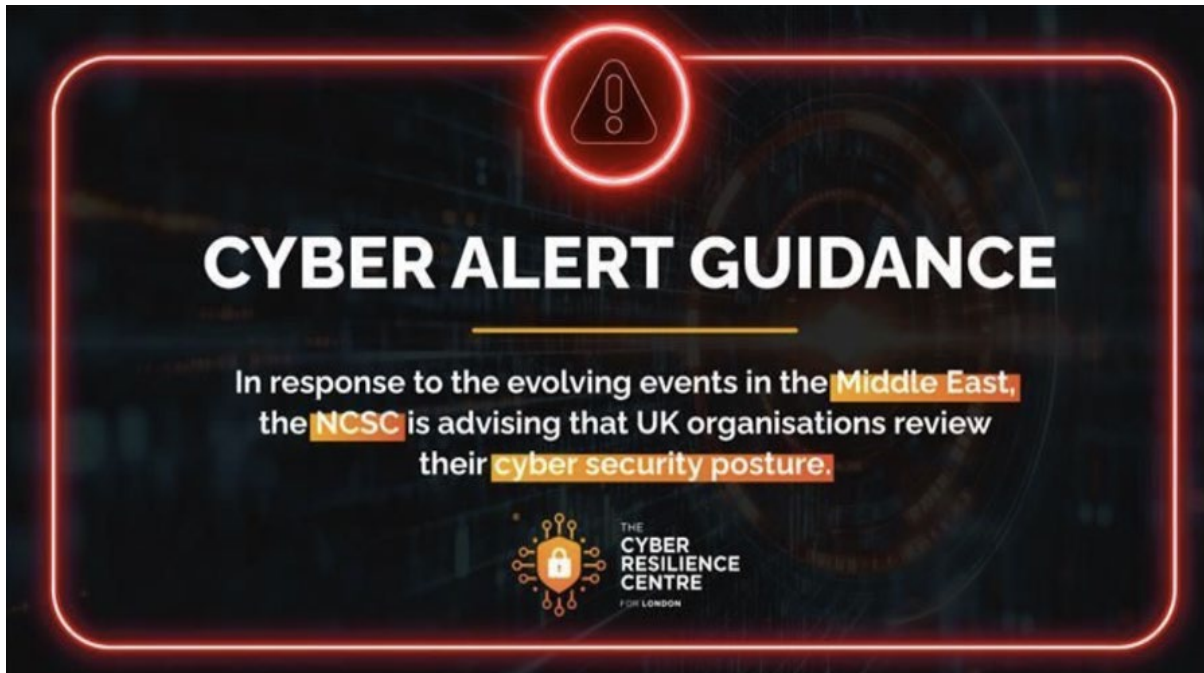
THE
CYBER
RESILIENCE
CENTRE
FOR LONDON



FAIRER
WESTMINSTER



Police and NCSC Alert Distribution



Supported distribution of timely and relevant alerts to organisations regarding emerging threats from both policing, and most recently from the NCSC in response to events in the middle east.

Distribution of this alert by the 9 CRCs resulted in 600+ businesses or third sector organisations booking Security Awareness Training.

Cyber PATH students provide a range of services



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.



Web Application Assessment

This service assesses your website and web services for weaknesses.



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.



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.

Service outputs

- Final report provided after each technical delivery
- Issues highlighted using a traffic light risk system
- Includes clear, actionable recommendations
- Written for non-technical audiences
- Organised into easy-to-follow sections with explanations
- Can be shared with internal IT or external partners for implementation





Cyber PATH – Police & Academia



CYBER PATHTM
POLICE & ACADEMIA
TALENT HORIZONS

Building an elite talent pipeline

Each of the nine Cyber Resilience Centres (CRCs) across England and Wales works closely with its **local universities** to handpick a unique and **talented cadre of students**, who work alongside senior Cyber Security Practitioners and police officers to deliver high-quality and tailored cyber resilience services to smaller organisations.

- Unique paid programme
- Comprehensive induction and training
- Baseline Personnel Security Standard vetting (UK OFFICIAL information and assets)
- Experienced cyber practitioners (ISO/IEC 27001 Lead Implementers), and police officers

Cyber PATH case study

Organisation: Black Country Woman's Aid

Sector: Third Sector

Service: Security Awareness Training (multiple sessions)



**Black Country
Women's Aid**

we listen, we support, we care



“Due to the scale of the charity, Security Awareness Training is something our IT provider couldn't deliver in a **cost-effective manner**, so I reached out to the West Midlands CRC to see how we could make use of the Cyber PATH services to deliver the training to all of the staff...

...the ultimate benefits for the whole organisation are limitless as now our staff take responsibility for their own cyber security and are very conscious of all the different permutations of what cyber security awareness means.”

Sara Ward, CEO, Black Country Woman's Aid



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON

Police-led, Business-focused



LONDON
Boroughs' Joint Network

londonplus



**London Communities
Emergency Partnership**





THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



london plus



**London Communities
Emergencies Partnership**



New frontiers in cybercrime: Defending against AI-driven voice impersonation





New frontiers in cybercrime

Artificial Intelligence

Voice cloning

Social engineering

Phishing





New frontiers in cybercrime

AI tools can generate an indistinguishable clone of a target voice with only few seconds of reference audio. This technology is emerging emergency as a way to bypass authorization protocols.

Establish “safe phrases”: Agree on offline verbal passwords with key family members, trustees, or executives.

Identify tone shifts: Listen for unusual gaps, monotonic cadences, or lack of standard vocal tics.

Verify externally: Hang up the phone and dial the person back on their saved mobile phone number.



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



LONDON
Boroughs Faiths Network

london plus



**London Communities
Emergency Partnership**



What does **good** look like?





What does good look like?

From the **police perspective**

- Most criminals target the vulnerability, not the business or charity
- Most cybercrimes are not sophisticated, but opportunistic
- Phishing remains the biggest risk area, criminals will continue to exploit “us”
- “I’m too small to be a target”, or “not important enough” are misconceptions
- No cost cyber awareness training, resources and services are available
- Implementing Cyber Essentials and the five control domains will make you resistant to the most common cyber attacks
- It’s not just your money or data: it’s your reputation, operations and interdependencies & your staffs emotional wellbeing and mental health



What does good look like?

Security Awareness Training - Ensure Security Awareness Training is embedded and effective

- Great option for all businesses to make staff more aware of the threats
- Covers topics including phishing, social engineering, password hygiene, social media conduct, and ransomware.
- Passkeys requiring user approval for logon access across digital services
- Where a service does not support a passkey then a password manager to create stronger passwords paired with two-step verification
- Create Incident Response and Business Continuity Plans
- Review, update and publicise your policies – BYOD, WFH, Reporting etc
- Test for vulnerabilities
- **Cyber Essentials** or **Cyber Essentials+** Certification
- Understanding regulatory and legal changes e.g. Cyber Security and Resilience Bill



Our support for the Third Sector

Small to Medium Sized Organisations (Up to 250 employees)

- Membership of their regional CRC
- All the support and guidance offered to organisations
- A range of fully funded cyber services delivered by the Cyber PATH programme

Larger Third Sector Organisations (Over 250 employees)

- Membership benefits of the regional CRC (excluding Cyber PATH services)
- Support to help you encourage SMEs in your supply chain to join their regional CRC
- Your supply chain SMEs then receive all the benefits of CRC membership, setting them on a path to better cyber resilience



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



london plus



**London Communities
Emergency Partnership**



Reporting Cybercrime and Fraud



Cyber Crime and Fraud Reporting



Cyber Crime and Fraud Reporting

reportfraud
.police.uk

Choose the right service for your situation:

- Report Fraud is not an emergency service; in an emergency you should **dial 999**.
- If the crime involves your bank account or credit card, always contact your provider first.
- Face-to-face crime which involves a local suspect, can be dealt with by your local police by **dialling 101**.



When to contact Report Fraud

- Report Fraud makes it easy and quick to report non-emergency fraud and cyber crime.
- You can also tell us about a **suspicious call, letter, text or email** even if you haven't lost any money.

Report Fraud offers a live cyber reporting helpline, open **24/7** for businesses.

If you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress), please call **0300 123 2040** immediately.



THE
**CYBER
RESILIENCE
CENTRE**
FOR LONDON



london plus



**London Communities
Emergency Partnership**



Thank you & any questions?

It's free to join and all cyber services are fully funded

