THE
CYBER
RESILIENCE
CENTRE
FOR THE **WEST MIDLANDS**

A POLICE LED PARTNERSHIP
IMPROVING CYBER RESILIENCE IN BUSINESSES
IN THE WEST MIDLANDS REGION

Become a member today for FREE via
wmcrc.co.uk/membership

WHAT IS THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS (WMCRC)?

The Cyber Resilience Centre for the West Midlands is a police-led, not-for-profit partnership between academia and business aimed at improving cyber resilience in businesses throughout the West Midlands region. The WMCRC is part of a nationwide network of centres established across the country.

When it comes to cyber criminals, there's nothing **small** about small businesses. If you're open for business online, you could be open to cyber-attacks. Let us help your business stay ahead of cyber criminals via our free core membership.

DOES THE WMCRC OPERATE IN YOUR AREA?

The WMCRC supports businesses, charities and third sector organisations in the West Midlands region including, Warwickshire, West Mercia, Staffordshire, Shropshire, Hereford, and Worcestershire.

HOW CAN YOUR BUSINESS ACCESS THE WMCRC?

Sign up for FREE membership to receive practical and simple to follow guidance about cyber resilience via **wmcrc.co.uk/membership**

JOIN US

Our mission is simple, we exist to help businesses of all sizes (although we do have a focus on SME's, micro businesses, and sole traders) to better protect themselves in the fight against cybercrime.

FREE Core Membership

- **A free 30 minute review** with the centre's Head of Cyber and Innovation on your current cyber set up.
- **Access to free resources, tools and guidance** designed to help your business start its cyber security journey including resources from the National Cyber Security Centre.
- **A Board Toolkit** - Resources designed to encourage essential cyber security discussions between the Board and their technical experts.
- **A bi-weekly update** containing short tips and tricks.
- **10 Steps to Cyber Security -** The steps enable businesses to break down the task of protecting their cyber security, by looking at 10 key components.
- **Exercise in a Box,** a suite of exercises based around real world scenarios designed to allow businesses to test their response and approach to each given scenario.
- **Invites** to all WMCRC webinars, roadshows, and conferences.
- **A monthly newsletter** full of tips, tricks, and resources to help you tackle current cyber threats and trends.

Affiliate Membership £500

All Core membership features plus

- **Use of the WMCRC logo** on your website.
- **A listing** under "Who we work with" on WMCRC Website, including a link to your website.
- **Bespoke newsletter article** to make our offer available to your supply chain, including webinar participation if required.
- **One feature per year in our e-newsletter** to present your company's offering to our members.
- **One news article per year** written for your business's external channels on a trending cyber topic of your choice.
- **A member's breakfast networking event** to take place twice a year.
- **A half day cyber security awareness session,** tailored to your business (worth £500).

Gold Membership £1000

All Core and Affiliate membership features plus

- **10% discount** on student services.
- **Two social media releases** about your membership, your company's offer, and your contribution to WMCRC.
- **One additional entry into e-news** to present your company's offering to our members.
- **A member's breakfast networking event** to take place twice a year.

Platinum Membership £1500

All Core, Affiliate and Gold membership features plus

- **15% discount** on one of our cyber services.
- **One joint event per year** to a target audience.
- **An introduction to our Trusted Partner network** to discuss shared agendas and business opportunities.
- **A one-month WMCRC social media campaign,** based on NCSC guidance to align with your own objectives and marketing strategy.
- **A member's breakfast networking event** to take place twice a year.

CYBER RESILIENCE SERVICES

SECURITY AWARENESS TRAINING
The training is focussed on those with little or no cyber security or technical knowledge and is delivered in small, succinct modules using real world examples.

CORPORATE INTERNET DISCOVERY
This service may be used to learn what is being said on the internet about an organisation, what information employees are releasing or if there are any damaging news stories, social media posts or associations.

INDIVIDUAL INTERNET DISCOVERY
The information gathered in this type of discovery might be used to support pre-employment checks, to manage potential threats to a Director of an organisation or their families, or to understand more about a specific person of interest.

REMOTE VULNERABILITY ASSESSMENT
Remote vulnerability assessments are focussed on identifying weaknesses in the way your organisation connects to the internet. Service reporting will provide a plain language interpretation of the results and how any vulnerabilities might be used by an attacker, as well as simple instructions on how any vulnerabilities might be fixed.

INTERNAL VULNERABILITY ASSESSMENT
The service will scan and review your internal networks and systems looking for weaknesses such as poorly maintained or designed systems, insecure Wi-Fi networks, insecure access controls, or opportunities to access and steal sensitive data.

WEB APP VULNERABILITY ASSESSMENT
This service assesses your website and web services for weaknesses. The service reporting will describe in plain language, what each weakness means to your business and the risks associated with each. Service reporting will include plans and guidance on how to fix those weaknesses.

SECURITY POLICY REVIEW
This service offers a review of your current security policy, how it is written and how it implemented.

CYBER BUSINESS CONTINUITY REVIEW
This service offers a review of your business continuity planning and the resilience of your organisation to cyber-attacks such as ransomware or when attackers take control of your core systems.

PARTNER RESOURCE SUPPORT
Student resource will be used to fill temporary resource gaps, support extended resource requirements to support projects, or during incident response.