THE
CYBER
RESILIENCE
CENTRE
FOR THE **EAST MIDLANDS**

EMCRC Community
Information Pack

CONTENTS

Welcome to **The Cyber Resilience Centre for the East Midlands** Community

Congratulations on taking your first step to strengthening your organisation's resilience against cyber crime by requesting our information pack.

Cyber crime and online fraud are a real threat to any business regardless of size or sector, costing dearly in terms of money, time, reputation and sometimes even customers. Now for the good news: effective cyber resilience practice doesn't have to be complicated or expensive and can not only save your business valuable resources but can enhance your business opportunities, enabling you to win government or other supply chain contracts which - without achieving certain standards - you may not be eligible for.

This information pack provides you with access to national guidance on cyber security, free online resources and toolkits and a tabletop exercise to assess your business resilience plans against a cyber-attack.

Once you have read your information pack and utilised the guidance and tools available, you may identify gaps where you feel you need more support from the EMCRC community. If you are unsure what additional support might be right for your business our EMCRC team can help guide you. We exist to help you to protect your business, as well as support you with your risk management and business resilience.

If you think that's too good to be true, take a look at our Community Pledge at *www.emcrc.co.uk/community-pledge*

As part of our commitment to you, we are proudly offering the following for free:

- ✓ Free cyber health assessment to help strengthen your current business set up.
- ✓ Regular newsletter and up-to-date scam alerts and fraud notifications, including sector specific bulletins.
- ✓ Access to our uniquely affordable services, delivered by our trained cyber specialists.
- ✓ Free and easy-to-follow cyber security exercises and toolkits from the National Cyber Security Centre for you to run with your employees.
- ✓ Access to all EMCRC webinars and events.

Who makes up **The Cyber Resilience Centre for the East Midlands**

The EMCRC began its journey in January 2020. Led by policing and facilitated by Business Resilience International Management (BRIM), we have followed a structured modular programme based on a highly successful model that had previously been established for over 9 years in Scotland.

We work in structured partnership with regional policing, academia, businesses, third and public sector organisations through a variety of ways;

MEET THE TEAM

The EMCRC is made up of a team of dedicated police officers and staff from local police forces who are here to support you.

Meet the full team at *www.emcrc.co.uk/meet-the-team*

OUR BOARD

We have established a Board of Directors and Strategic Advisors who are responsible for setting the strategic direction of the centre and to make sure that we serve the needs of our local business communities. The Board is made up of East Midlands Police Officers, Police and Crime Commissioners and business leaders who all share a passion to protect businesses in the region and reduce business-related crime.

Meet our Board at *www.emcrc.co.uk/meet-the-team*

OUR CYBER ESSENTIALS PARTNERS

Our Cyber Essentials Partners are official providers of Cyber Essentials Certification and have been accredited by the Information Assurance for Small and Medium Enterprises Consortium (IASME).

Our Cyber Essentials Partners can help your organisation achieve Cyber Essentials and Cyber Essentials Plus Certification.

Achieving Cyber Essentials allows you to guard your organisation against the most common cyber threats and helps you to demonstrate your commitment to cyber resilience for your customers and staff.

Meet our Cyber Essentials Partners at *www.emcrc.co.uk/cyber-essentials-partners*

OUR CyberPATH STUDENTS

Each of the nine Cyber Resilience Centres (CRCs) across England and Wales work closely with 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.

Find out how our students can help you at *www.emcrc.co.uk/security-awareness-training*

Identifying your Cyber Risks

Good Cyber Resilience practice is what a business needs to have in place to minimise the risks of being hit by a successful cyber-attack.

Imagine receiving a ransom note demanding money in cryptocurrency and you being unable to gain access to your company's network.
Could you contact your staff? Could you contact your clients? How could you operate? When could you get back to business as usual? How much would it cost? Who would you call to fix it? Do you need to report it? How do you deal with the impact longer term?

Hopefully, you can answer these questions satisfactorily. Whatever the answer though, there will be a cost, in terms of time, revenue and potentially reputation and customers.

If you can't answer these questions successfully - how can you help minimise risk to keep your company in business? A lot of these attempted attacks can be prevented by understanding the individual risks and vulnerabilities of your business. By putting the right mitigations in place, you can ensure you are as protected as you can be.

To identify your cyber security risks, take a look at these 3 key areas:

Technologies

Using outdated software, having no firewalls, no anti-virus, no encryption and no data backups, mean you are maximising the chances of a successful attack, and limiting your chances of recovery.

Processes

Do you have a current risk register and the necessary policies, processes and procedures in place to mitigate those risks? Does your organisationhave insurance which covers you for losses? Do you have processes in place to verify the phishing email which lands asking your company to make new payments to a new unfamiliar bank account?

People

You can have the best next generation firewall in the world protecting your network, but if an employee opens an attachment on a phishing email, the firewall won't help. People are your strongest asset or weakest link. Empower them with knowledge and the confidence to spot these low-level attacks.

As with any risk to your business, you cannot 100% guarantee it won't happen, BUT you can reduce the risks significantly.

If you have a plan about what to do if things go wrong, then that is cyber resilience! It is an ability to bounce back with minimal disruption.

We aim to help you avoid common attacks and demonstrate that you take cyber security seriously, protecting the data that you hold.

If you would like to take advantage of your Free Cyber Health assessment, contact us at *www.emcrc.co.uk/contact-us*

The Cyber Health Assessment will address your current set-up and highlight relevant services to address any obvious risks or your concerns.

Subject to eligibility and officer availability, certain sectors will qualify for a free on-site security review conducted by one of our trained police cyber security professionals. Once you register your interest, a member of the EMCRC team will get back to you.

Your **Free Resources, Tools and Support**

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 advice.

The EMCRC has put together some of the top resources the NCSC has produced to make it easy for your business to access them.

Just click on the headings to get more information:

SMALL BUSINESS GUIDE

www.ncsc.gov.uk/collection/small-business-guide

An easy-to-understand guide with five key steps you can take to manage your cyber security risks.

SECURING YOUR SOCIAL MEDIA CHANNELS

www.ncsc.gov.uk/guidance/social-media-protect-what-you-publish

Social media is a wonderful way to stay in touch with family, friends and keep up to date on the latest news. It is important to know how to manage the security and privacy settings on your accounts, so that your personal information remains inaccessible to anyone but you.

CYBER ACTION PLAN

www.ncsc.gov.uk/news/cyber-aware-action-plan

Answer a few questions and get a personalised list of actions to help you or your business improve your cyber security.

10 STEPS TO CYBER SECURITY

www.ncsc.gov.uk/collection/10-steps-to-cyber-security

Guidance is designed to help organisations protect themselves in cyberspace. It breaks down the task of defending your networks, systems, and information into its essential components, providing advice on how to achieve the best possible security in each of these areas.

EXERCISE IN A BOX

www.ncsc.gov.uk/information/exercise-in-a-box

An online tool which helps organisations test and practice their response to a cyber-attack. It is completely free, and you do not have to be an expert to use it. It includes two exercises, a technical simulation, and a tabletop exercise. You just need to register for an account.

NCSC BOARD TOOLKIT

www.ncsc.gov.uk/collection/board-toolkit

Boards are pivotal in improving the cyber security of their organisations. The Board Toolkit has been designed to help board members get to grips with cyber-security and know what questions they should be asking their technical experts.

Continued >>

Your **Free Resources, Tools and Support** (continued)

CYBER SECURITY TRAINING FOR STAFF

www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

Your staff are your first line of defence against a cyber-attack. The NCSC has developed an e-learning training package 'Stay Safe Online: Top Tips for Staff' to help educate your staff on a range of key areas including phishing, using strong passwords, securing your devices, and reporting incidents.

EARLY WARNING SERVICE

www.ncsc.gov.uk/information/early-warning-service

Helps organisations investigate cyber-attacks on their network by notifying them of malicious activity that has been detected in information feeds.

ACTIVE CYBER DEFENCE (ACD)

www.ncsc.gov.uk/section/active-cyber-defence/introduction

This programme seeks to reduce the harm from commodity cyber attacks by providing tools and services that protect against a range of cyber security threats.

CYBER INFORMATION SHARING PLATFORM (CISP)

www.ncsc.gov.uk/section/keep-up-to-date/cisp

This is a joint industry and government initiative run by the NCSC and a good place for network defenders to find help and speak with like-minded people.

OTHER RESOURCES

The EMCRC has put together some top resources from other areas to make it easy for your business to access them:

FREE CYBER HEALTH ASSESSMENT

www.emcrc.co.uk/contact-us

Our free Cyber Health Assessment provides a review of your current cyber set-up that will help your business, charity or third sector organisation address any gaps in your cyber security.

HAVE I BEEN PWNED

www.haveibeenpwned.com/DomainSearch

Have you set up your organisation for domain search protection with Have I been pwned? A free service that's worthwhile to keep you notified about any of your domain emails featuring in data breaches which would be a precursor for business email compromise (really important if 2fa is inactive) and phishing email campaigns.

INFORMATION SECURITY POLICIES

www.sans.org/information-security-policy

In collaboration with information security subject-matter experts and leaders who volunteered their security policy knowledge and time, SANS has developed and posted a set of security policy templates for your use.

Continued >>

Your **Free Resources, Tools and Support** (continued)

GET READY FOR CYBER ESSENTIALS

www.iasme.co.uk/cyber-essentials/about-cyber-essentials/

Cyber Essentials is an effective, Government-backed baseline scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber-attacks.

Cyber-attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a burglar trying your front door to see if it's unlocked. Our guidance is designed to prevent these attacks.

Sometimes, organisations are unsure about where to start to prepare for Cyber Essentials. This simple tool is a series of questions that have been developed to lead you through the main parts of the Cyber Essentials requirements. If there are areas where you need to put more controls in place, you will get a link to guidance about how to make those changes. At the end of this process, you will get a list of actions outlining what steps you need to take to prepare for Cyber Essentials and links to specific guidance on those actions.

TEST FILTERING CHECK

www.swgfl.org.uk/services/test-filtering

Check your internet connection blocks child abuse & terrorist content.

POLICE CYBERALARM

www.cyberalarm.police.uk

Police CyberAlarm is a free tool backed by policing and funded by the Home Office to help your business understand and monitor malicious cyber activity. Police CyberAlarm monitors the traffic seen by a member's connection to the internet. It will detect and provide regular reports of suspected malicious activity, enabling organisations to minimise their vulnerabilities.

Stay **Connected**

Our team at the EMCRC are friendly, knowledgeable and on hand for you to contact for support and guidance should you need us.

To stay up to date with the latest news from us and the wider security industry, please follow us on our social media channels.

FOLLOW US

LinkedIn

Twitter

Facebook

Instagram

In the coming weeks, we will be in touch to see how you are making use of the information and resources that we have provided to see if you need any additional support from us.

The Cyber Resilience Centre for the East Midlands is looking forward to working in partnership with you and your organisation to make the East Midlands region a more cyber resilient place to live, work and do business.

THE
CYBER
RESILIENCE
CENTRE
FOR THE **EAST MIDLANDS**

Reporting **Cyber Crime**

If you or someone else is in immediate danger or risk of harm dial 999 now.

Anyone can find themselves the victim of cyber crime.

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

This service is available 24 hours a day, 7 days a week.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

REPORTING A CYBER ATTACK WHICH ISN'T ONGOING

Please report online to Action Fraud, the UK's national reporting centre for fraud and cybercrime. You can report cybercrime online at any time using the online reporting tool, which will guide you through simple questions to identify what has happened. Action Fraud advisors can also provide any help, support and advice you may need. Alternatively, you can call Action Fraud on 0300 123 2040 (textphone 0300 123 2050).

When you report a fraud to Action Fraud, you are given a police crime reference number and your case will be referred to the National Fraud Intelligence Bureau (NFIB), which is run by the police.

In some cases, the police and other law enforcement agencies may want to contact you for further details, so it's important that you provide your correct contact details and keep any relevant information about the crime.

Although the police cannot investigate every report individually, the information you provide will aid them. The police use your information to build up intelligence about cybercrime, which includes who is committing what crimes and against whom. This contributes to making the UK a more hostile place for cybercriminals to operate and helps to keep other potential victims safe.

When you report to Action Fraud, you can also choose to have your details passed on to Victim Support, a national charity that helps those affected by crime. If you take up this option, you will then be contacted by someone from the charity and offered free and confidential emotional support and practical help.

For more information on how to report different forms of cyber crime, visit ***www.emcrc.co.uk/reporting-cybercrime***

THE
CYBER
RESILIENCE
CENTRE

FOR THE **EAST MIDLANDS**