THE
CYBER
RESILIENCE
CENTRE
FOR THE EAST MIDLANDS

Cyber Resilience Services

CONTENTS

1 About Cyber PATH

2 Cyber PATH Process

3 Our Support

4 Cyber Resilience Services

5 Stay Connected

6 Reporting Cyber Crime

About Cyber PATH

It could be time to further boost your resilience by taking some action.

So far in your step-by-step information packs, we've provided you with information about the cyber risks you need to consider and given you free resources to get your resilience journey started.

Take the next step by undertaking one of our uniquely affordable services to help identify any vulnerabilities you may have.

ABOUT Cyber PATH

Cyber PATH, coordinated centrally by the National Cyber Resilience Centre Group (NCRCG), employs exceptional students from universities across the country who are looking to shore up the nation's defences against cybercrime and gain vital experience in a commercial setting.

We've interviewed and selected the best talent from the region, working with undergraduate and postgraduate students. They're passionate, background checked, and insured – and they work under the supervision of our Cyber PATH experienced national cyber specialists, delivering each service using industry-standard tools and techniques.

The Centre provides nine cyber resilience services, designed especially for smaller business, including the self-employed and third sector. Our services are regularly reviewed with government and law enforcement cybercrime data, to ensure that we help you improve your resilience from the types of cyber threat that are most common for your type of organisation.

CyberPATH allows smaller businesses to access practical, affordable and bespoke support from the EMCRC at a highly subsidised rate.

WHY STUDENTS?

Cyber PATH allows small and medium businesses to access practical and bespoke support from the EMCRC at an affordable rate.

Students are paid appropriately for their work whilst ensuring they have the flexibility and time to balance the programme's activities with their university studies. With unique workplace experience and BPSS vetting, Cyber PATH greatly enhances students' employability upon graduation.

This means that whilst you benefit from affordable priority cyber resilience services, tailored to suit smaller organisations, we can prepare and speed up the UK's talent with high quality work experience to have them ready to ensure law enforcement, defence and critical national infrastructure can fill their skills gap to protect us all at work and at home.

Cyber PATH **Process**

HOW DOES IT WORK?

We will arrange a conversation with you to agree your cyber concerns and needs; we'll then follow up with a more detailed conversation with one of the technical team to explore the relevance and extent of the work you require, which can vary depending on the complexity of your own organisation and systems.

We'll then give you an obligation-free quotation for the work, and if you want to engage our team, we'll find the right person from our Cyber PATH team to deliver that work in a timely and professional manner. The work is overseen by our experienced supervisors. We always provide full reporting, and a presentation of findings, at which you can ask questions and develop a more detailed understanding. And if we uncover any high-risk issues during the process, we'll let you know immediately, and help you navigate how to remediate these.

HOW WE CAN SUPPORT YOU

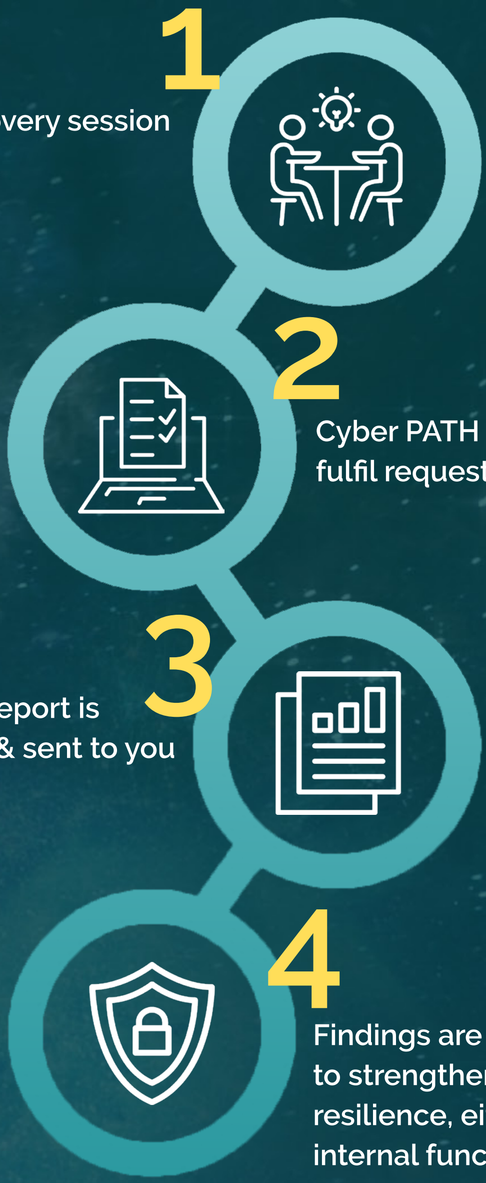
Part of our support service here at EMCRC is to help you learn more and discover what's relevant for your organisation as well as protect you from buying things you don't need.

We are a not-for-profit company and police led. Our trusted team can help you identify which service is most suited to you to begin with, support you through that process, and if at the end of it you need a commercial provider for wider support, then we can also point you in the direction of our Partners, which are government approved Cyber Essentials scheme certifiers.

We are a friendly and approachable team. We are a jargon-free zone and genuinely here to help protect organisations in the East Midlands from the ever-expanding threat that is cybercrime.

Conversation is a great place to start, if you like to ask us some questions, we can help you find the answers.

If you wish to find out more, you can contact us at *www.emcrc.co.uk/contact-us*.



1 Initial discovery session

2 Cyber PATH team fulfil requested

3 Findings report is prepared & sent to you

4 Findings are implemented to strengthen your cyber resilience, either by your internal function or external partners

Cyber Resilience **Services** *(Click on the headings for more information)*

SECURITY AWARENESS TRAINING

Provides employees with a basic but effective understanding of their cyber environment and the confidence to recognise and draw attention to any potential security issues.

FIRST STEP WEB ASSESSMENT

An initial assessment of your website to highlight its most pressing vulnerabilities. It is considered a light-touch review in comparison to the fuller Web App Vulnerability Assessment offered.

CORPORATE INTERNET DISCOVERY

A comprehensive review of publicly available information about your business using internet search and social media tools.

INTERNAL VULNERABILITY ASSESSMENT

Identifies any weaknesses in your internal networks and systems, such as insecure WiFi networks and access controls, or opportunities to steal

INDIVIDUAL INTERNET DISCOVERY

A comprehensive review of publicly available information about a potential or existing employee employee using internet search and social media tools.

WEB APP VULNERABILITY ASSESSMENT

A complete assessment of your website to highlight any vulnerabilities and their potential risk to your business.

REMOTE VULNERABILITY ASSESSMENT

Identifies any weaknesses in the way your organisation connects to the internet.

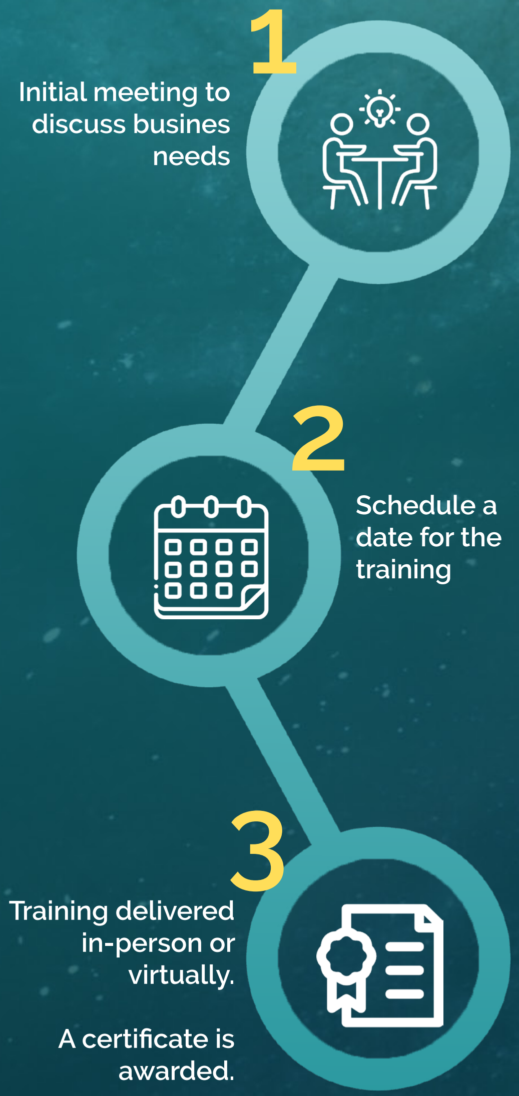
SECURITY POLICY REVIEW

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

CYBER BUSINESS CONTINUITY REVIEW

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

Cyber Resilience **Services**



1

Initial meeting to discuss busines needs

2

Schedule a date for the training

3

Training delivered in-person or virtually.

A certificate is awarded.

WHAT IS SECURITY AWARENESS TRAINING?

Based on the National Cyber Security Centre's Small Business Guide, Security Awareness Training provides employees with a basic but effective understanding of their cyber environment and the confidence to recognise and draw attention to any potential security issues.

Topics include:

- Recognising social engineering
- How to protect against the different 'ishings' e.g. spear phising, vishing, email phishing and smishing
- The importance of strong passwords
- Social media conduct
- Handling a ransomware attack

WHO IS IT FOR?

Everyone in your workforce. Employees are the first layer of cyber defence in any business so ensuring they can spot common cyber security issues or risks is essential.

The training is aimed at those with little or no technical knowledge and delivered in small, succinct modules supported by real-world examples that are relevant to the context of your business.

HOW LONG DOES A SESSION TAKE?

Each training session typically lasts 2.5 hours however this timing is flexible should you require a shorter or longer session.

Our trainers are highly knowledgeable, personable and strive to create an environment whereby all employees feel comfortable and able to ask questions.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.

Security Awareness Training

Cyber Resilience **Services**

WHAT IS A FIRST STEP WEB ASSESSMENT (FSWA)?

A FSWA is a light-touch assessment of your website's security which highlights the most pressing weaknesses, for example sensitive data exposure or vulnerable and outdated components.

Our work is non-intrusive and should have no effect on your website's performance. All we need is the website address you would like us to assess.

WHO SHOULD GET A FSWA?

Any business that uses a website or web services.

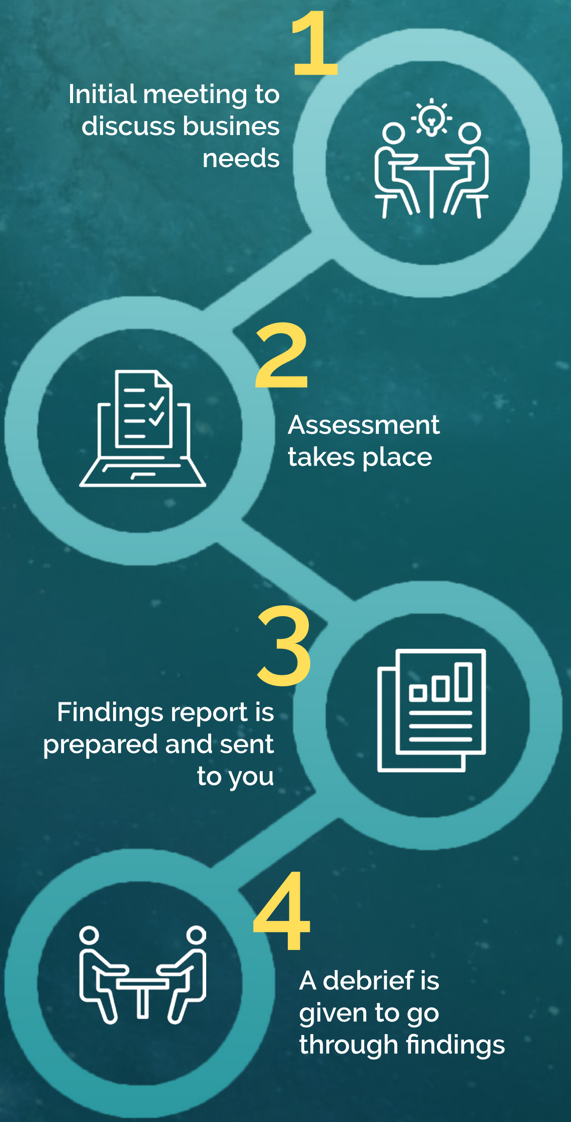
WHAT ARE THE BENEFITS TO MY BUSINESS?

- Informs you of high-level risks to your website;
- Acts as a first step to minimise the chance of a criminal breaching your website and causing financial or operational disruption;
- Provides you with reassurance that you are doing what you can to protect your services for the benefit of your customers and reputation.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.

First Step Web Assessment



1 Initial meeting to discuss busines needs

2 Assessment takes place

3 Findings report is prepared and sent to you

4 A debrief is given to go through findings

Cyber Resilience **Services**

WHAT IS AN INTERNAL VULNERABILITY ASSESSMENT (IVA)?

An IVA looks at what a cyber criminal could see and do if they were to gain access to your business's internal network.

Our team will send you a small computer to plug into your internal network and will carry out a scan and thorough review to identify any weaknesses e.g. insecure WiFi networks and access controls, or opportunities to steal sensitive data.

If any weaknesses are found, we will rate the risk that they pose to your business and can advise you on next steps you can take with your internal IT team or an external partner to address them.

WHO SHOULD HAVE AN IVA?

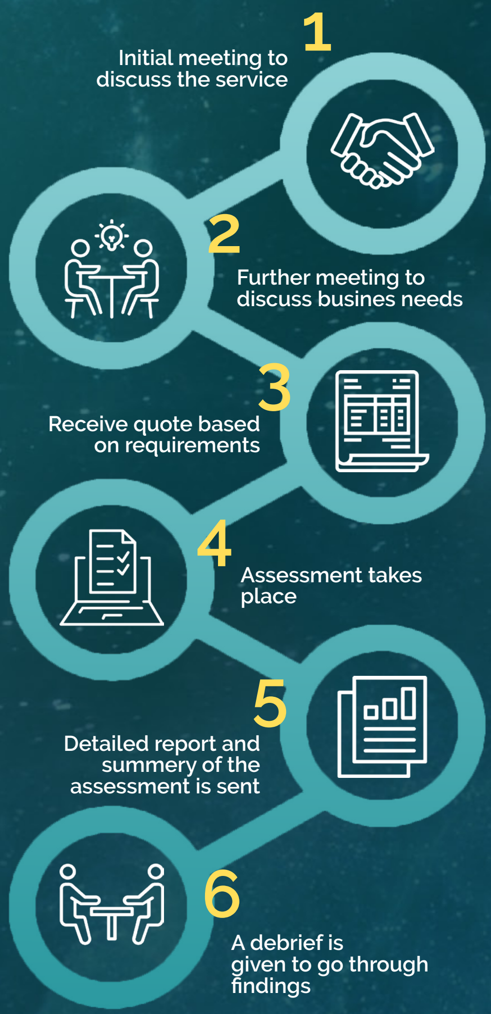
Any business with an internal network or systems. A business that operates with one computer, or only uses cloud services, is unlikely to require this service but we would be happy to have an initial discussion with you to confirm if it would be of benefit.

WHAT ARE THE BENEFITS TO MY BUSINESS?

- Informs you of the impact a cyber criminal could have if they attacked your network;
- Gives you the insights you need to fortify your network based on risk;
- Provides you with reassurance that you are doing all you can to protect your customers, your supply chain and your employees.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.



1 Initial meeting to discuss the service

2 Further meeting to discuss busines needs

3 Receive quote based on requirements

4 Assessment takes place

5 Detailed report and summery of the assessment is sent

6 A debrief is given to go through findings

WHAT IS A WEB APPLICATION VULNERABILITY ASSESSMENT (WAVA)?

A WAVA involves looking at your website or web services to determine if there are any weaknesses which could be exploited by cyber criminals.
To do this, we use a combination of automated scans and manual passive testing which would not impact on the performance of your web services.
If any weaknesses are found, we rate the risk that they pose to your business and can advise you on next steps you can take with your internal IT team or an external partner to address them.

WHO SHOULD HAVE AN WAVA?

Cyber criminals commonly run scans to look for known weaknesses in business' websites or web services. A WAVA is therefore something all businesses with any online presence should consider.

WHAT ARE THE BENEFITS TO MY BUSINESS?

- Reduces the chance that a criminal can breach your website and cause financial or operational disruption, protecting against loss of data, money and time;
- Provides you with reassurance that you are doing all you can to protect your customers, your supply chain and your employees.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.

Vulnerability Assessments

Cyber Resilience **Services**

Internet Discovery

WHAT IS INTERNET DISCOVERY?

Our Internet Discovery service provides a comprehensive review of publicly available information about your business, employees, suppliers or prospective partners, using internet search and social media tools.

It is primarily focused on identifying any information that could be used by cyber criminals to craft an attack however is tailored to each business' individual objectives and concerns.

There is no interaction with any organisation or individual and no intrusive measures or tools are employed.

WHO IS IT FOR?

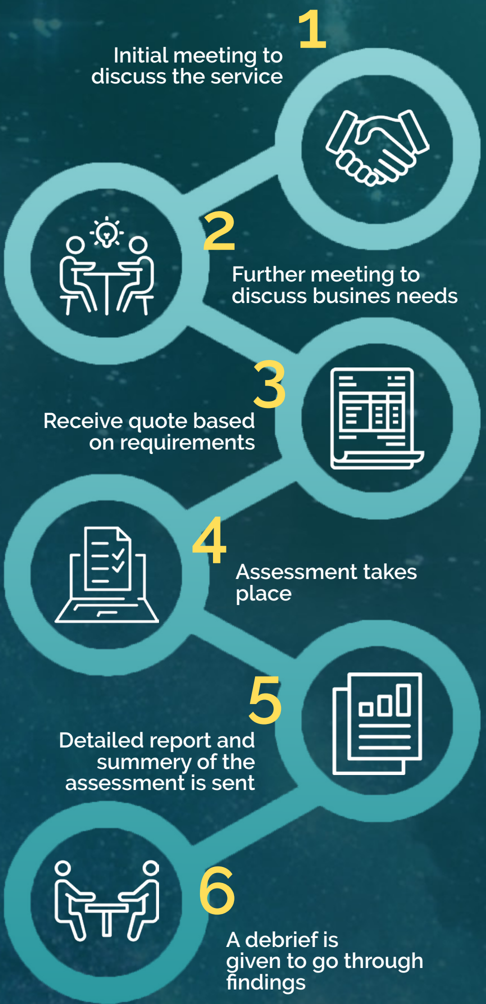
Any business with an online presence, or whose staff are active online, will benefit from having a firmer understanding of what is being shared about them.

WHAT ARE THE BENEFITS TO MY BUSINESS?

- Understand more about your online security posture and how likely it is to draw the attention of cyber criminals;
- Identify if your employees are sharing personal or business sensitive information which puts them or your organisation at risk;
- Undertake high-level due diligence on your suppliers, competitors or prospective partners.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.



1 Initial meeting to discuss the service

2 Further meeting to discuss busines needs

3 Receive quote based on requirements

4 Assessment takes place

5 Detailed report and summery of the assessment is sent

6 A debrief is given to go through findings

Continuity Policy Review

WHAT IS A CYBER BUSINESS CONTINUITY POLICY REVIEW?

It is essential to ensure that your business can continue to function should it be impacted on by a cyber attack.

As part of this service, our team reviews your existing cyber business continuity policy to determine how your business would respond to a cyber incident and if you have an appropriate plan in place to best protect your business and customers. For example, who assesses whether a cyber attack has taken place or whether it is an IT failure? Is it clear who would lead the subsequent response? Is there a way for you to contact customers if your network has gone down?

Our review is modelled on the international business continuity management systems standard 'ISO/IEC 22301:2019'.

WHO IS IT FOR?

Any business with an existing cyber business continuity policy.

WHAT ARE THE BENEFITS TO MY BUSINESS?

- Clear understanding of whether your cyber business continuity plan is fit for purpose; loss of data money and time;
- Analysis against the key ISO standards so you can see where your plan is strong or where it needs improvement;
- Plain language report which is accessible to all;
- Opportunity to dscuss your review with our \ cyber professionals.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.

Cyber Resilience **Services**

Cyber Security Policy Review

WHAT IS A CYBER SECURITY POLICY REVIEW?

Our team reviews your organisation's cyber security policy to ensure that you're communicating your goals and objectives effectively to employees – and that these are based on sound practice and considerations.

As a basis, we use the internationally recognised information security management standard 'ISO/IEC 27001:2022', however we believe in a personalised approach. We take the time to understand your organisation's specific context and tailor our review to your unique needs.

By doing so, we empower you to have meaningful conversations and make informed decisions regarding cyber security and information security. It is essential that you have an accessible yet robust policy in place which all employees can refer to and, most importantly, understand.

WHO IS IT FOR?

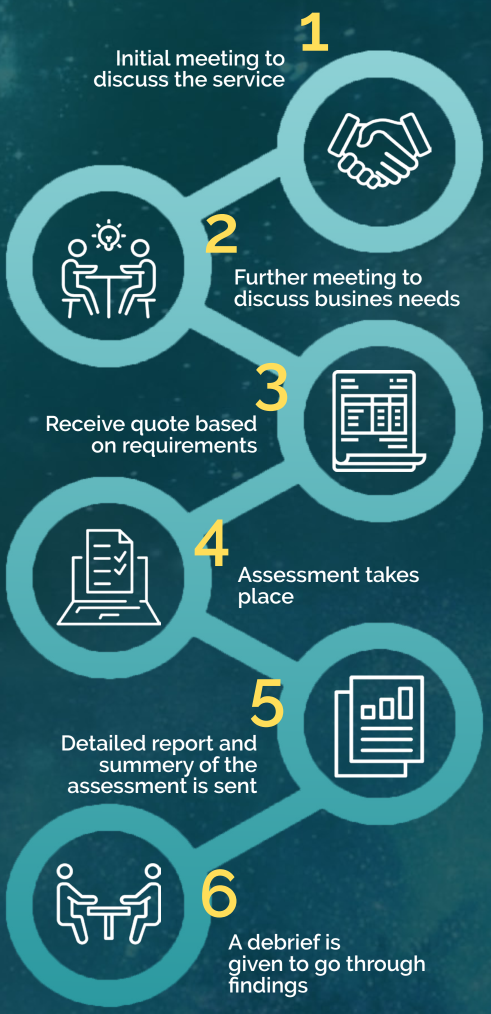
Any business with a cyber security policy. This policy may not include 'cyber' in its name but may instead be called Information Security Policy or Email Policy.

WHAT ARE THE BENEFITS TO MY BUSINESS?

- Clear understanding of whether your cyber security policy is fit for purpose;
- Analysis against the key ISO standards so you can see where your plan is strong or where it needs improvement;
- Plain language report which is accessible to all;
- Opportunity to discuss your review with our cyber professionals.

HOW MUCH DOES IT COST?

Each service we offer is tailored to suit the needs of the business we are working with.



1 Initial meeting to discuss the service

2 Further meeting to discuss busines needs

3 Receive quote based on requirements

4 Assessment takes place

5 Detailed report and summery of the assessment is sent

6 A debrief is given to go through findings

HOW DO YOU FIND OUT MORE?

If any of our services take your fancy, email *engagement@nationalcrcgroup.co.uk* to set up an initial discussion with one of our Cyber PATH team members and receive a free, no obligation quote.

ABOUT THE NATIONAL CYBER RESILIENCE CENTRE GROUP (NCRCG)

The National Cyber Resilience Centre Group (NCRCG) is a strategic collaboration between the police, government, private sector and academia to help strengthen cyber resilience across the nation's small and medium-sized enterprise community. Key to our reach are nine cyber resilience centres which operate across England and Wales to provide affordable, high-quality cyber resilience services to local organisations. These services are delivered by NCRCG's Cyber PATH student team, under the supervision of senior cyber security practitioners.

Learn more about the Cyber PATH programme by visiting *https://nationalcrcgroup.co.uk/cyber-path/*

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**