

Policing Led - Business Focussed.



THE **EASTERN CYBER RESILIENCE CENTRE**

www.ecrcentre.co.uk

Detective Inspector Fiona Bail

Detective Supt Paul Lopez



What is the ECRC?

- Home Office supported project
- Collaboration between Policing, Industry Experts and Academia
- Not for Profit Limited company
- Membership focussed - with free of charge membership

Aim:

To increase the cyber resilience of Small and Medium businesses



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE SOUTH WEST



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



THE
**CYBER
RESILIENCE
CENTRE**
FOR WALES



THE
**CYBER
RESILIENCE
CENTRE**
FOR GREATER MANCHESTER



THE
**BUSINESS
RESILIENCE
CENTRE**
FOR THE NORTH EAST



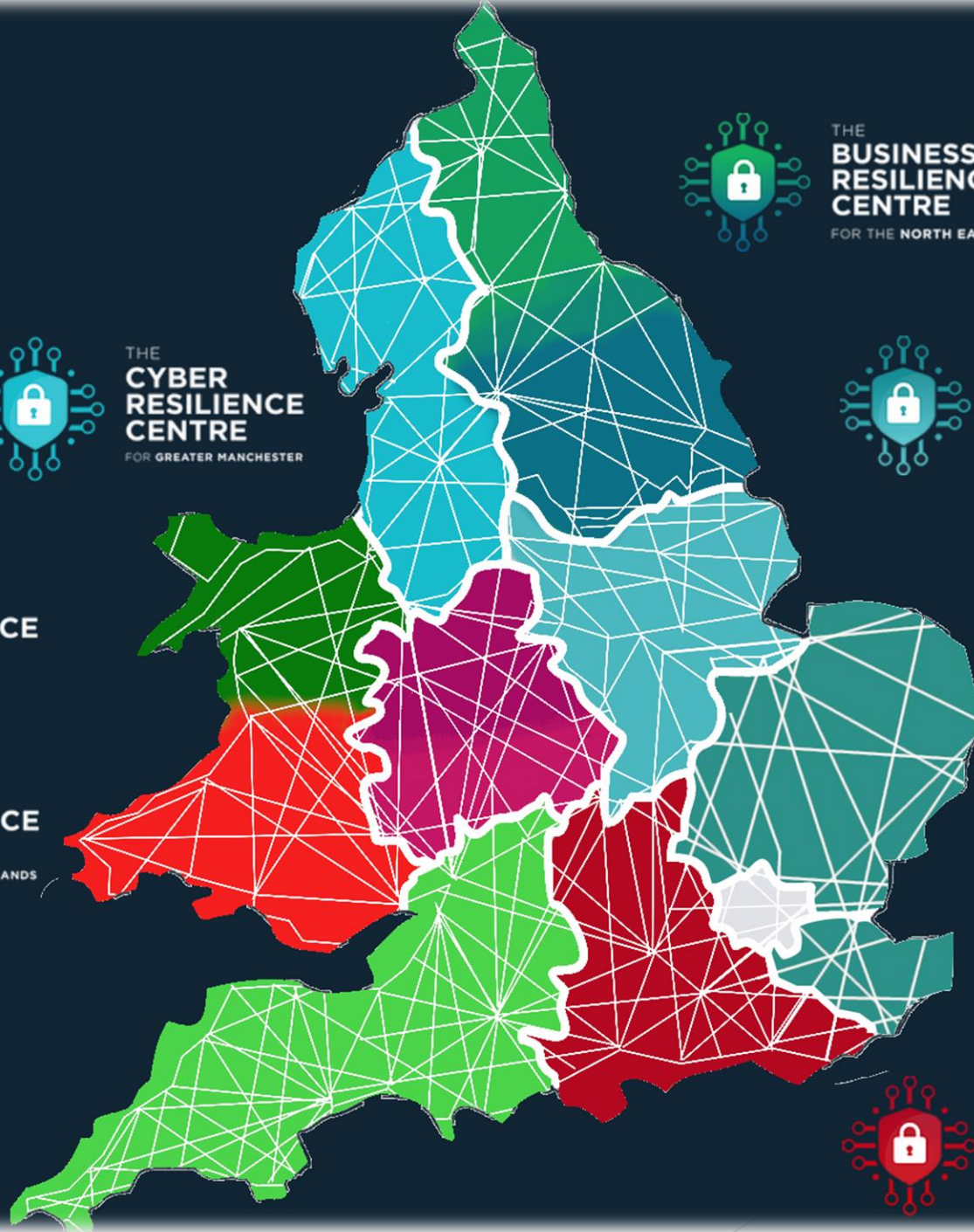
THE
**CYBER
RESILIENCE
CENTRE**
FOR THE EAST MIDLANDS



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE EAST



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE SOUTH EAST



Why have the Cyber Resilience Centres been set up?

Cybercrime is increasing

1.5 million organisations fell victim to cyber crime in 2019 (Beaming's five years in cyber security)

25% of all UK businesses and an increase from the 13% in 2015

The est. cost of cyber crime to the UK business - £21bn per year
(Detica report, Office of Cyber Security and Information Assurance, Cabinet office)

£233.3m loss in Eastern England between Jan - July 2021 (Action Fraud)

Most cybercrime is for one thing - MONEY, either directly (theft) or indirectly (ransomware, selling data)

“I'm too small to be a target”

- ▶ Criminals target vulnerabilities

Video Case Study

- ▶ Password was compromised via a data breach where the same password was used
- ▶ Gained access to email system
- ▶ Sent change of account details out without firm knowing
- ▶ Criminals got paid
- ▶ Customers lost money and trust

Potentially

The email that was sent to the customers could have a malicious attachment which then infects the customers networks

43% of SMBs lack any type of Cyber Resilience Plan

1 Small Business in the UK is successfully hacked every 19 seconds

Hackers target **VULNERABILITIES** not organisation size

4 in 10 SMEs say they would struggle to recover from data loss.

1 in 4 SMEs admit they wouldn't be able to recover any data.

41% of UK consumers claim they will never return to a business after a data breach



Free of charge core membership

Provides members with:

- ▶ Access to national **guidance** on cyber resilience, free online **resources** and **toolkits**.
- ▶ Regular updates from the ECRC team including the latest information about emerging **threats** in our region.
- ▶ **Contact** from a member of the ECRC to discuss your current cyber resilience and discuss areas to consider.
- ▶ A “**little steps**” journey - receive one email a week about one cyber resilience consideration.

The screenshot displays the CRC Membership website with a teal and white color scheme. At the top, there are three service cards: 'Security Awareness Training' (with a photo of people in a meeting), 'Corporate Internet Investigation' (with a magnifying glass over a keyboard), and 'Individual Internet Investigation' (with a photo of hands holding a document). Below these is a 'WHAT WE DO' section with three columns: 'Knowledge & Protection' (with a padlock icon), 'Membership' (with a star icon), and 'Skills & Talent' (with a lightbulb icon). Each column lists specific services and includes a 'HOW WE DO IT' link. At the bottom, there are three more service cards: 'Security Policy Review' (with a photo of a hand writing on a notepad), 'Cyber Business Continuity Review' (with a photo of a hand holding a paper), and 'Partner Resource Support' (with a photo of a hand holding a document). Each card includes a brief description and a 'Find Out More' link.

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.
[Find Out More](#)

Corporate Internet Investigation
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.
[Find Out More](#)

Individual Internet Investigation
The information gathered in this type of investigation 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.
[Find Out More](#)

WHAT WE DO

Knowledge & Protection
• We coordinate cyber risk and protection information between policing and business
• We help business understand what's relevant to them
• We help you access NCSC free resources
[HOW WE DO IT](#)

Membership
• We provide regular e-updates
• We deliver affordable testing and training services
• We are a place to find trusted and accredited suppliers
[HOW WE DO IT](#)

Skills & Talent
• We provide real world experience for emerging university cyber talent
• We develop real world commercial skills for students
• We provide transferrable skills opportunity for veterans
[HOW WE DO IT](#)

Security Policy Review
This service offers a review of your current security policy, how it is written and how it is implemented.
[Find Out More](#)

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.
[Find Out More](#)

Partner Resource Support
Student resource will be used to fill temporary resource gaps, support extended resource requirements to support projects, or during incident response.
[Find Out More](#)



Trusted Partners & Cyber Essentials Scheme



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

Think of it as an annual MOT for your businesses' cyber resilience.

Delivered by our Trusted Partners who are Accreditation Bodies within the Eastern region.





IASME
CONSORTIUM

Impact of Cyber Essentials



Security
Lancaster

Lancaster
University

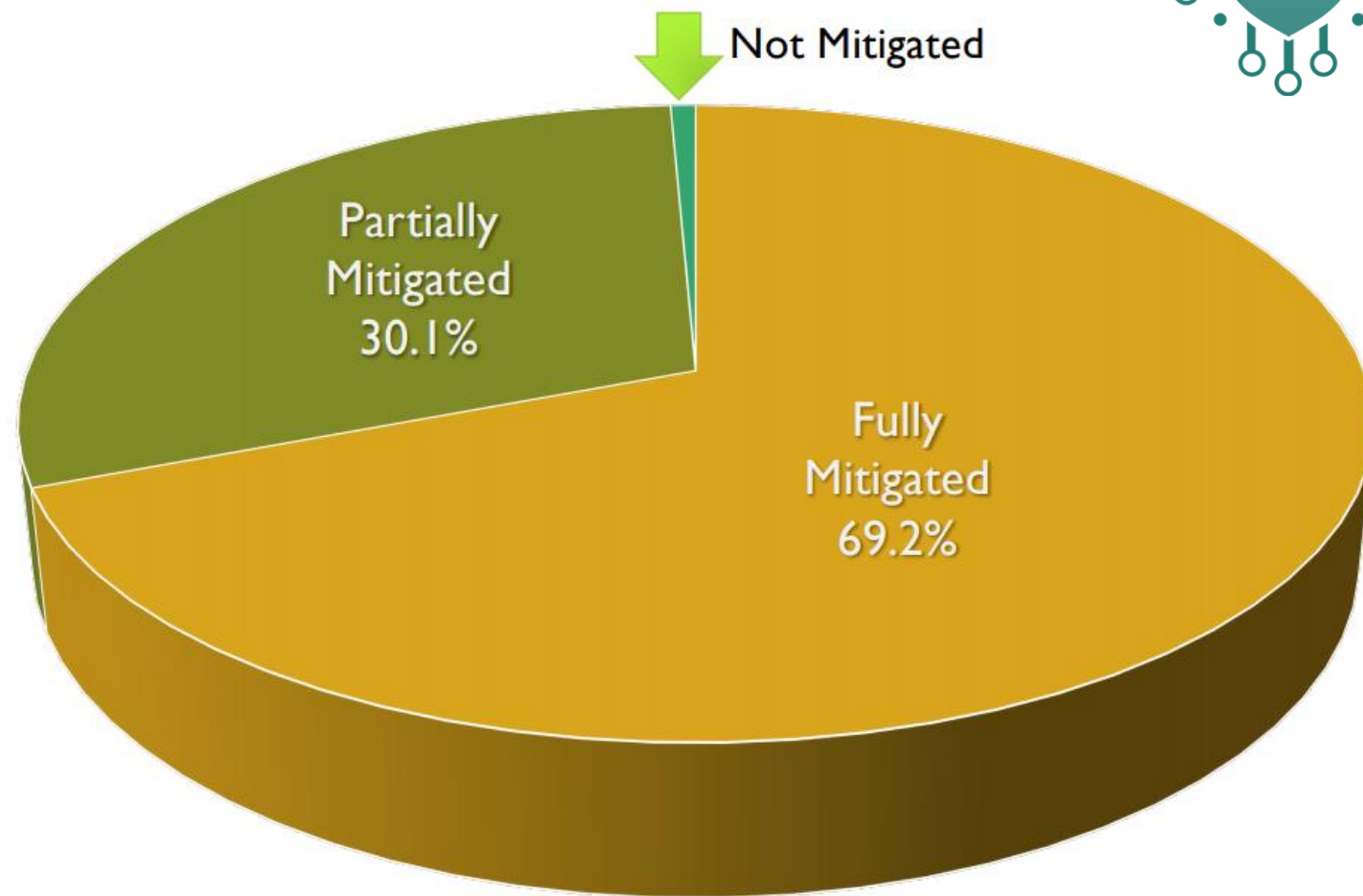


CYBER SECURITY CONTROLS EFFECTIVENESS

A Qualitative Assessment of Cyber Essentials

Attacks Mitigated

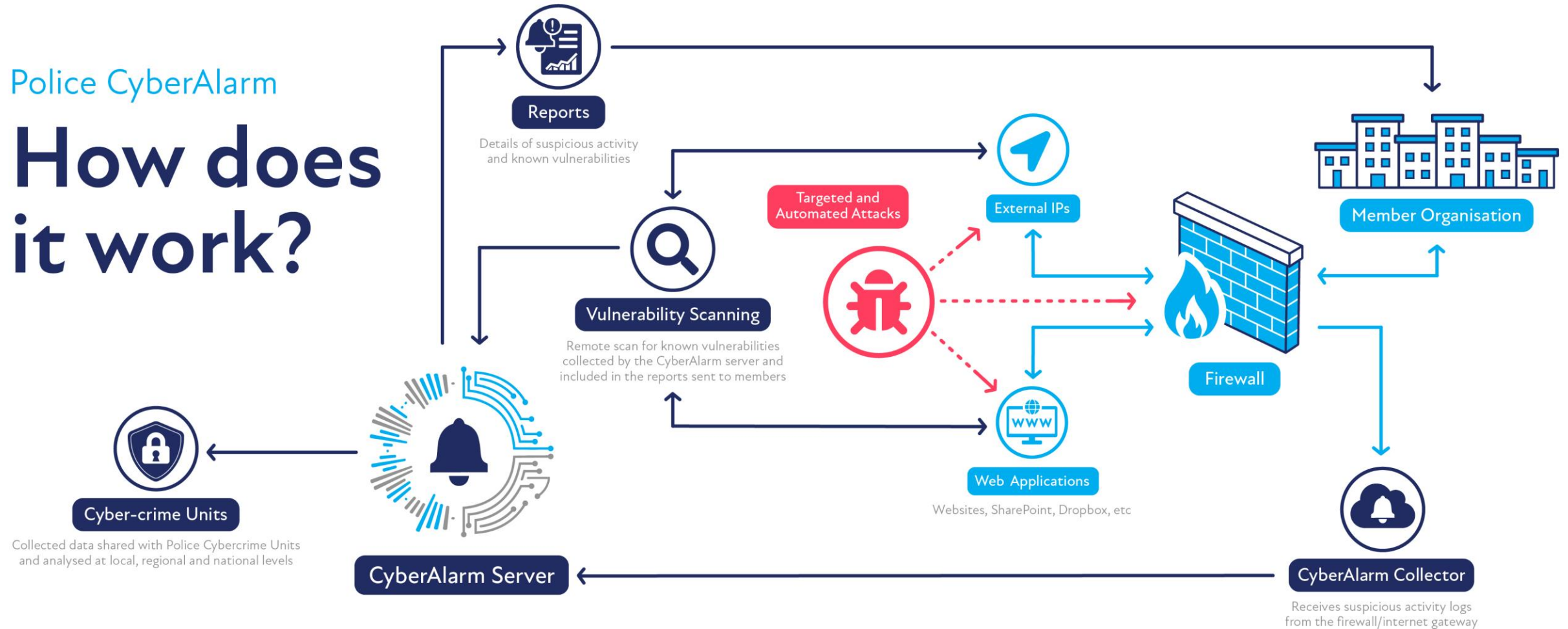
- Full 69.2%
- Partial 30.1%
- Not Mitigated 0.7%





Police CyberAlarm

How does it work?





Quick and Easy Tips for Cyber Resilience



DON'T USE THE
SAME PASSWORD
ACROSS MULTIPLE
ACCOUNTS



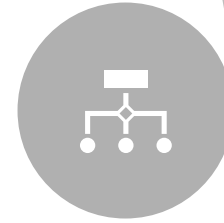
MAKE YOUR
PASSWORDS
COMPLEX - USE 3
RANDOM WORDS
OR A PASSWORD
MANAGER



ENABLE 2FA ON
ANY IMPORTANT
ACCOUNT
ESPECIALLY EMAIL
AND SOCIAL MEDIA



CHECK YOUR
CURRENT
EXPOSURE -
HAVEIBEENPWNED
.COM



REGISTER YOUR
DOMAIN WITH
HAVEIBEENPWNED
.COM



Affordable Student Services

A WIN-WIN

Provides **eight cyber resilience services**, designed especially for smaller business, including the self-employed and third sector.

Delivered through an innovative UK Talent Pipeline Programme, where the UK leading universities in cyber skills, partner with policing and the private sector to provide commercial training and oversight for students to deliver this work.

Businesses - benefit from affordable priority cyber resilience services

Cyber Industry - prepare and speed up the UK's talent ready for graduation

Students - benefit from high-quality work experience, with real world situations and expert guidance from some of the best in the field



Affordable Student Services

- ▶ **Internal Vulnerability Assessment**

Find out how much damage an attacker could do if they did manage to breach your network or launch an attack from the inside. The objective of an Internal Vulnerability Assessment is to safeguard the network's assets that could be exploited to interfere with the confidentiality, availability, and integrity of your network.

- ▶ **Remote Vulnerability Assessment**

We can scan your network remotely, like an attacker might, and see if there are obvious weaknesses present which they might choose to exploit.

- ▶ **Web Application Vulnerability Assessment**

How secure is your website? Does it contain vulnerabilities just waiting to be exploited? Our assessments can help identify these weaknesses so you can fix them.



Affordable Student Services

► Individual Internet Investigation

Harvesting online information about senior team members in your business can help an attacker craft a convincing phishing email. Find out what exists online about you and your team, and how it could be used in an attack.

► Corporate Internet Investigation

Find out what information an attacker can gather about your business and how it can be used in a cyber-attack.



Affordable Student Services

- ▶ **Security Policy Review**
Find out how robust your current cyber security policies are and what can do to improve them.
- ▶ **Cyber Business Continuity Exercise**
A cyber tabletop exercise helps identify issues in the Cyber aspects of your company's current business continuity plan, including emergency response plans, disaster recovery plans and backup integrity testing.
- ▶ **Security Awareness Training**
Ensure your staff are aware of the risks associated with cyber and how to protect themselves and your business.



Summary

- ▶ The CRC is a new way of working for the police
- ▶ Cybercrime is a growing problem
- ▶ Most businesses don't realise that they are a target for cyber crime, but unfortunately if you are online, you are a target.
- ▶ If businesses do realise they are a target, they are unsure about where to start or who to trust.
- ▶ The ECRC is that starting point, with our free of charge membership to get businesses started on their cyber resilience journey.

The ECRC is here to help

Thank you for listening

Any questions?

DI Fiona Bail - Fiona.bail@ecrcentre.co.uk

<https://www.ecrcentre.co.uk>

<https://www.linkedin.com/company/the-cyber-resilience-centre-for-the-east>

<https://twitter.com/EasternCRC>