south east
Regional Organised Crime Unit

THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST

Case Study:
Regional Cybercrime Units: Developing a Holistic Approach to Identify and Respond to Emerging Cyber Crime

Chris White
Head of Cyber & Innovation
Police Detective Inspector

NPCC National Police Chiefs' Council | Home Office

Cybercrime Statistics

Teens **more likely to unlawfully hack** (5%) than smoke (3%) or have sex (2%)

Teens **more likely to unlawfully hack** (5%) than be in a gang (2%)

~1% of teenagers **sent a virus** at least once in previous 12 months

1 in 4 Teenagers admitted having **tried to compromise someone's account**

17 Average age of arrest for cyber crime

61% Of hackers started **before 16 yrs old**

83% rise in cyber frauds by those under 18 over three years

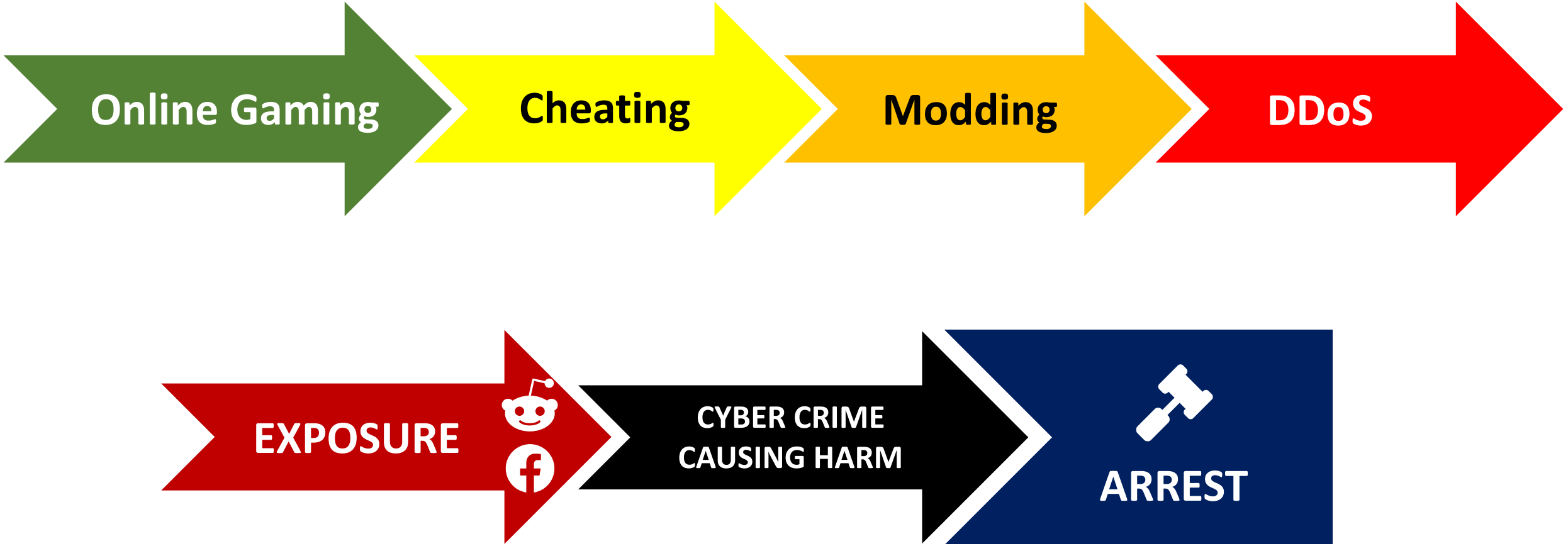
1 in 2 Businesses close within 6 months of a cyber attack

Helping people to make the right #CyberChoices

south east
Regional Organised Crime Unit

Pathways to Cyber Crime

Not all online gamers are cyber criminals, but when we find the cyber criminal we often find:



Enablers of Cyber Crime

Cyber Crime Services
'Off the Shelf' Hacking Tools

No fear of getting caught

Perceived as Victimless

Chat forums

Lack of understanding of law

Raising Awareness

Schools are the starting point, but in the South-East region alone:

- 1500+ Primary Schools
- 750+ Secondary Schools
- + Further and Higher Education…

The response requires:

- Educating schools – a holistic, multi-agency *Safeguarding* issue and not just Law Enforcement… a need to teach computer law and ethics
- Embedding computer misuse into Safeguarding processes
- Identifying individuals of concern and educating and diversion
- Deterring those who might be tempted to commit cybercrime

The Cyber Choices Team…

Identifies and educates

Deters and diverts

Manages the highest risk cyber offenders

Explores pathways into cybercrime

The Cyber Choices Team…

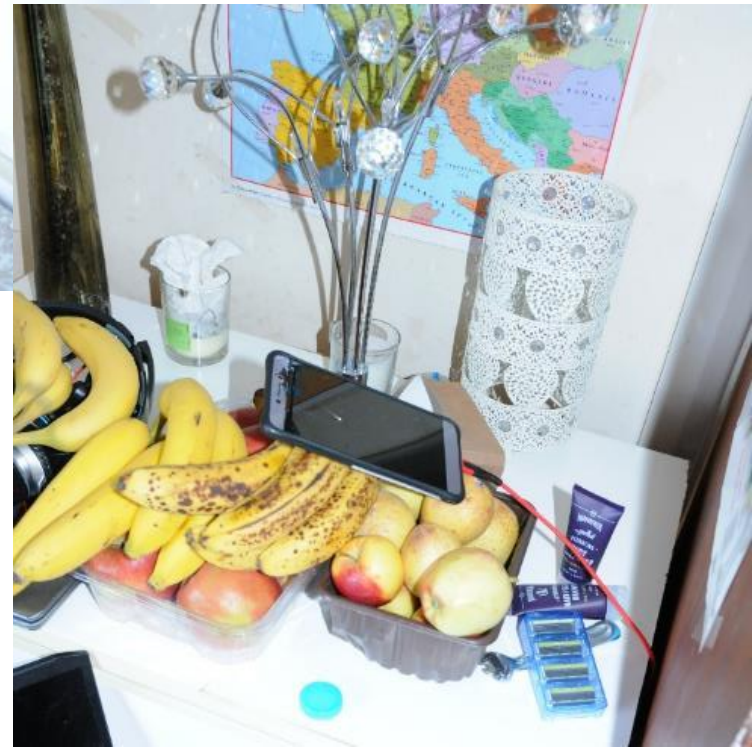
https://serocu.police.uk/cyber-choices/

CyberChoices@serocu.police.uk

March 2020 SEROCU were on call for Team Cyber UK

On Friday 13th, we got "THAT" call from TICAT


PROGESS
BITSUM25OFF
PREDATOR



M.O.

- Tested website's security for captcha / 2fa
- Brute forced those without, using sourced credentials and a script to report positive returns
- Would then manually log in on positive hits, make benefit
- Made DIY combo lists from various sources / youtube / forums

Important to note during Covid-19 crisis companies

were not

interested in supporting investigation

Had never seen the

sheer amount of legitimate internet traffic

hitting their sites just ordering food

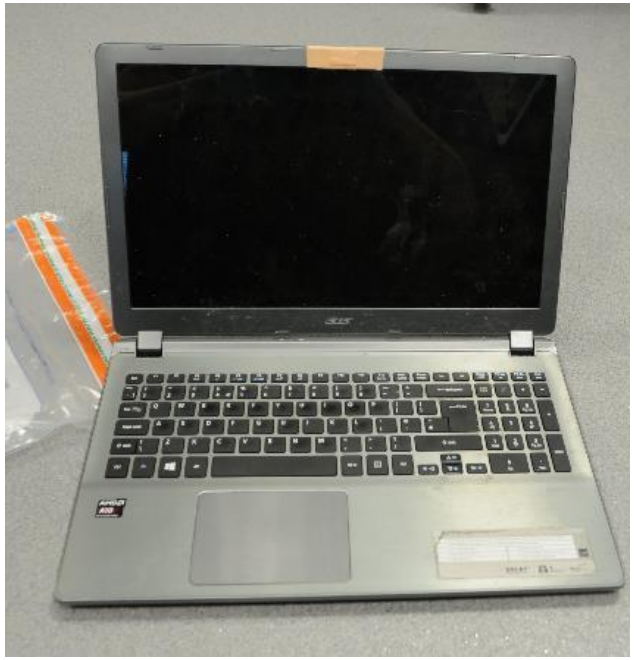
IT department's priorities were trying to

keep their companies and infrastructure online, they were in survival mode

1st laptop - 60,451,061 end users / 19 combos
2nd laptop - 15,948,788 end users / 43 combos

Total **76 MILLION+** compromised details
usernames & passwords / email & passwords

10,443,930 returned as unique to this operation



Action taken on 7,120,993 which was 68% of output

3,377 belonged to Government Addresses of which

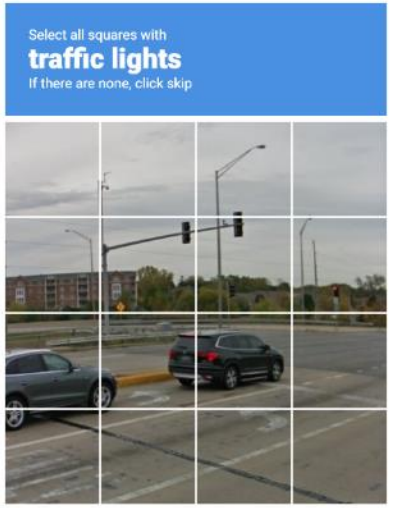
988 were NHS

10,008 were Universities

Time Line

1700 13/3/20	Initial contact from TICAT
1200 14/3/20	Deployed Assets
1330 14/3/20	Subject in custody
15-18/3/20	Digital Forensic work/Cyber Protect strategy
19/3/20	2nd Interview
23/3/20	Securing statements & evidence gathering
6/4/20	Submitted CPS Charging advice file

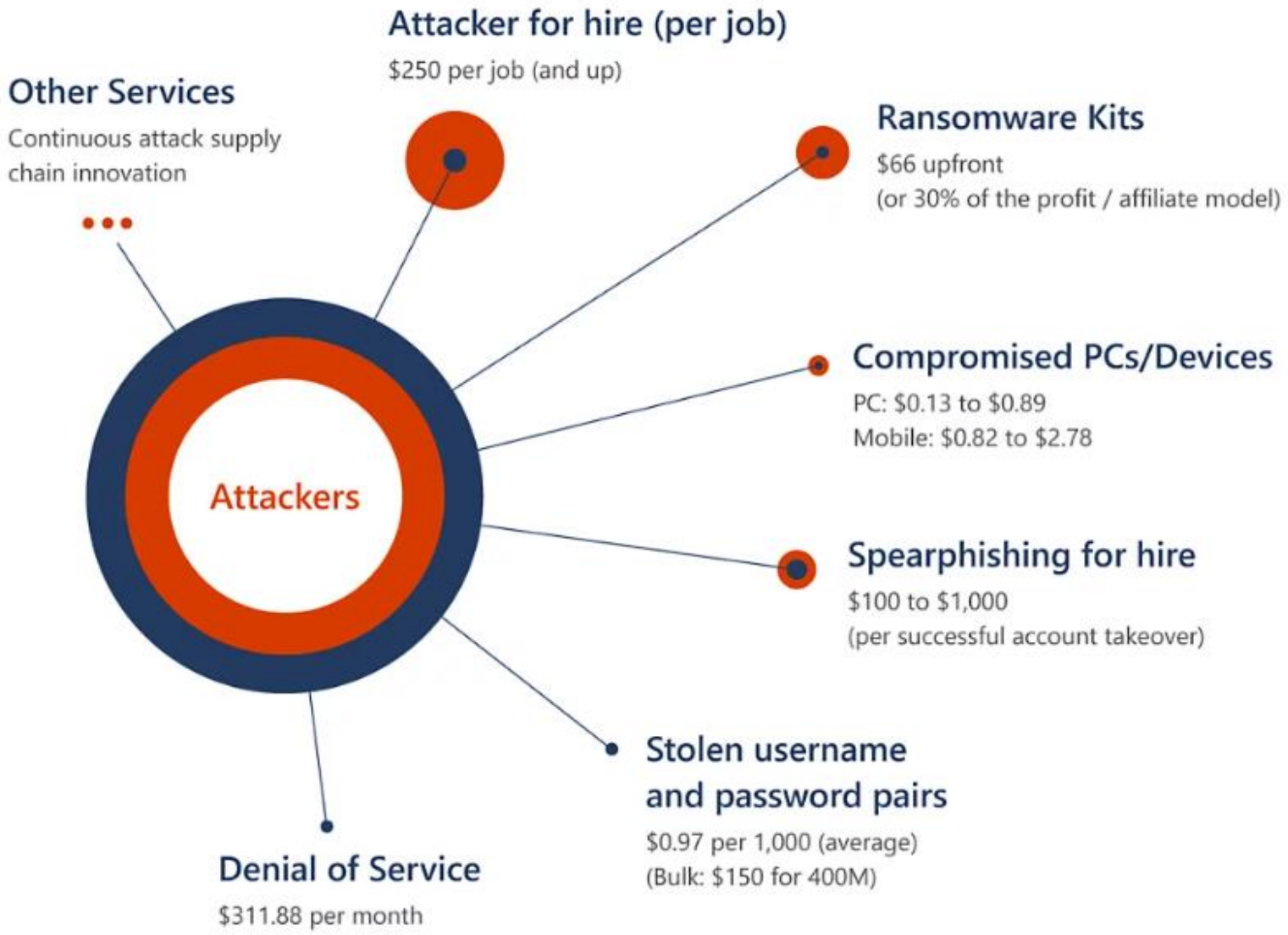
Mitigation



- Activate Google CAPTCHA on login endpoint
- Forced password changes on affected accounts
- Provided Info all affected with basic cyber mitigation
  - Password policy to be reviewed to increase to at least NCSC guidance 12 characters+ and complexity
  - Turning on or offering 2FA to end users
  - Create lockout policy

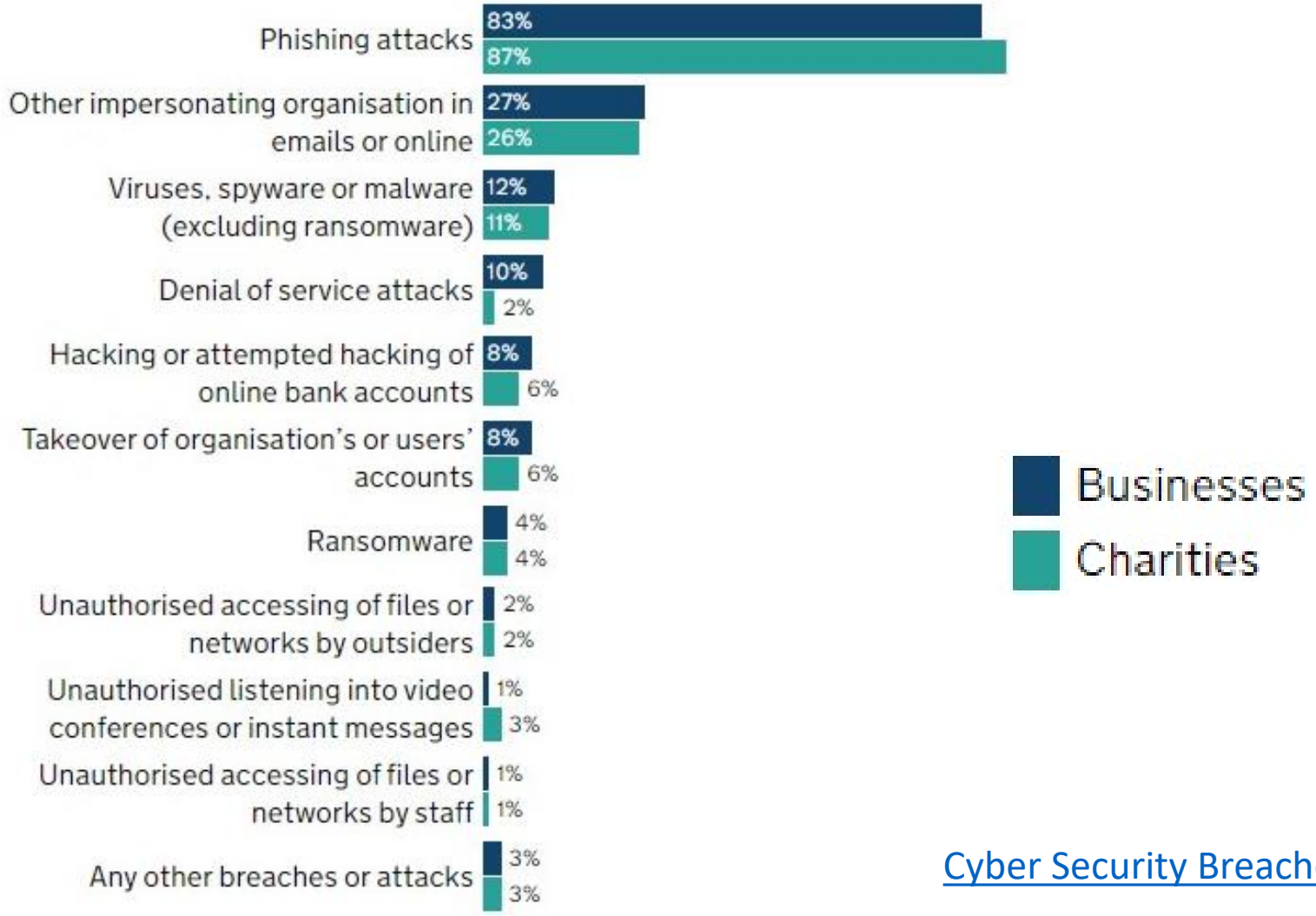
Current Threat

Average prices of cybercrime services for sale



[Microsoft Digital Defense Report]

Harm



[Cyber Security Breaches Survey 2022]

Risk

Password attacks	34,740 per minute
IoT-based attacks	1,902 per minute
DDoS attacks	19 per minute
Phishing attacks	7 per minute
SQL injection attacks	1 per minute
New threat infrastructure detections	1 every 35 minutes
Supply chain attacks	1 every 44 minutes
Ransomware attacks	1 every 195 minutes

Cyberthreat Minute: The scale and scope of worldwide cybercrime in 60 seconds

Fergus Falls Journal.com

It's in the bag

It's in the bag

Read more | Add your comment

FEATURED NEWS

Otter Tail Telcom internet services suffer 5 hour outage

Otter Tail Telcom internet services were limited or completely unresponsive since about 12:30 p.m. Monday. The outage was reportedly caused by a construction company accidentally ... Read more | Add your comment

Memoir recalls early days in the area | Add your comment

Moorhead boater accused of drowning buck, says he was

FEATURED OPINION

Vision of Lake Alice remains captivating

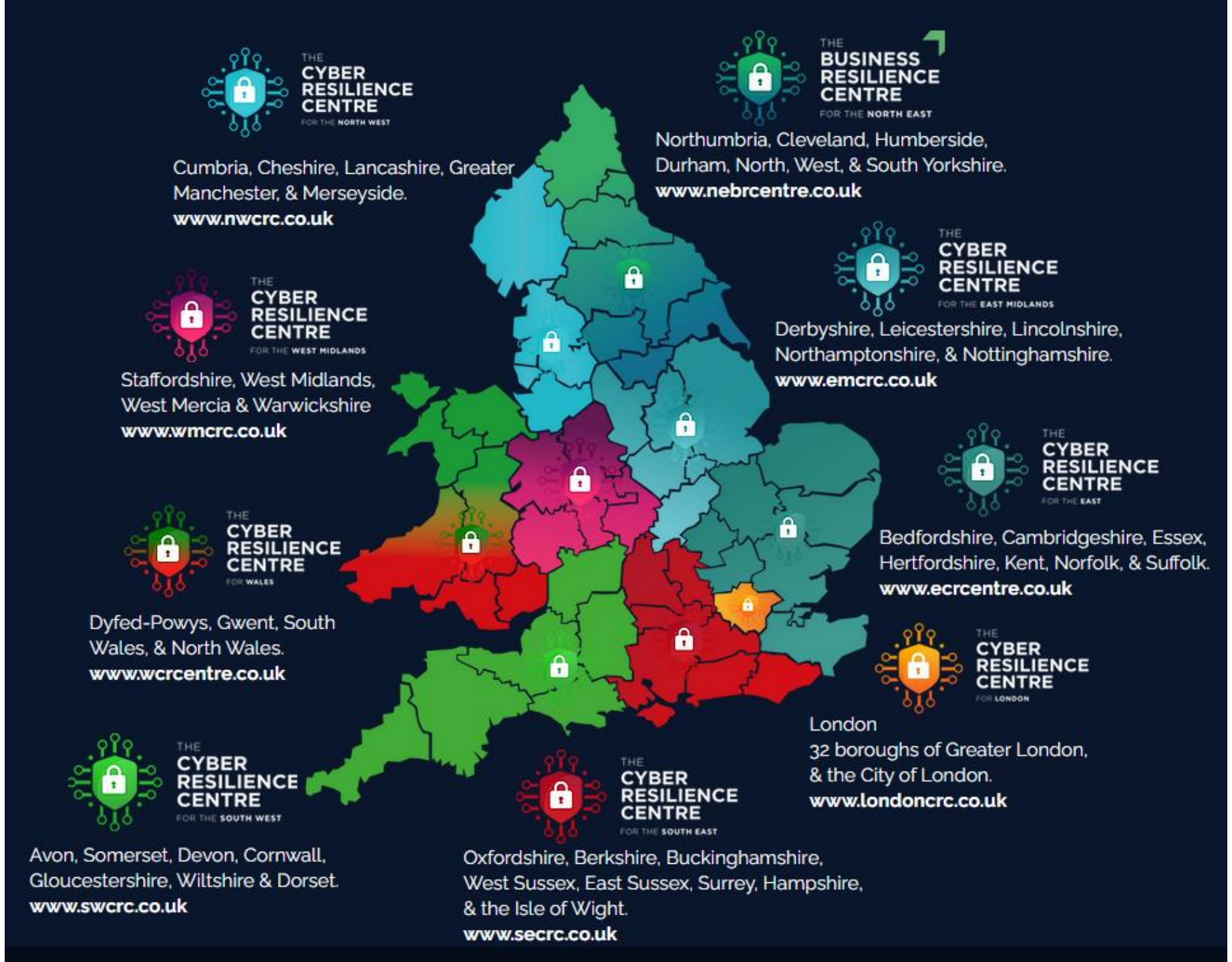
SOLE TRADERS. SMEs. THIRD SECTOR ORGANISATIONS.

BOOST YOUR CYBER RESILIENCE

- Consultancy in order to grow and strengthen the UK's resilience to online crime and cyber attacks
- Bridging the gap between police messaging and large cyber security provider's offerings
- Working with student talent to provide low cost services
- Provide guidance and support from leading law enforcement and industry experts to help take simple steps to protect their business from unscrupulous cyber criminals.

Police partnership aimed at improving #CyberResilience businesses -www.secrc.co.uk

THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST


THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST
Cumbria, Cheshire, Lancashire, Greater Manchester, & Merseyside.
www.nwcrc.co.uk
THE BUSINESS RESILIENCE CENTRE FOR THE NORTH EAST
Northumbria, Cleveland, Humberside, Durham, North, West, & South Yorkshire.
www.nebrcentre.co.uk
THE CYBER RESILIENCE CENTRE FOR THE EAST MIDLANDS
Derbyshire, Leicestershire, Lincolnshire, Northamptonshire, & Nottinghamshire.
www.emcrc.co.uk
THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS
Staffordshire, West Midlands, West Mercia & Warwickshire
www.wmcrc.co.uk
THE CYBER RESILIENCE CENTRE FOR THE EAST
Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Kent, Norfolk, & Suffolk.
www.ecrcentre.co.uk
THE CYBER RESILIENCE CENTRE FOR WALES
Dyfed-Powys, Gwent, South Wales, & North Wales.
www.wcrcentre.co.uk
THE CYBER RESILIENCE CENTRE FOR LONDON
London
32 boroughs of Greater London, & the City of London.
www.londoncrc.co.uk
THE CYBER RESILIENCE CENTRE FOR THE SOUTH WEST
Avon, Somerset, Devon, Cornwall, Gloucestershire, Wiltshire & Dorset.
www.swcrc.co.uk
THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST
Oxfordshire, Berkshire, Buckinghamshire, West Sussex, East Sussex, Surrey, Hampshire, & the Isle of Wight.
www.secrc.co.uk

Cyber Services

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

Individual Internet Discovery
Find out what exists about you or one of your senior team online and how this could be used against you

Security Awareness Training
Ensure your staff are aware of risks faced from Cyber and how to protect themselves and your business

Remote Vulnerability Assessment
Can an attacker breach your system remotely?

Internal Vulnerability Assessment
Find out how secure your network is once an attacker has managed to make a connection

Web Application Vulnerability Assessment
Find out what vulnerabilities exist, what risks they create for your business and how to fix them

Security Policy Review
Find out how robust your current Cyber Security Policies are

Cyber Business Continuity Exercise
A practical assessment tailored for your organisation to test your business continuity plan and its robustness facing cyber-attacks

Partner Resource Support
Student Resource will be used to fill temporary gaps, support extended resource requirements to support projects, or during incident response.

Start that #CyberEssentials journey be more resilient against a cyber attack

- Obtaining Cyber Essentials Certification is simple with minimal cost
- Assessed against 5 basic security controls
- A qualified assessor verifies that information
- Eligible companies entitled to FREE Cyber Insurance
- Implementing Cyber Essentials can stop the majority of Cyber Crime

IASME Consortium®
+
CYBER ESSENTIALS

south east
Regional Organised Crime Unit

THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST

Thank you for listening

Chris White, Head of Cyber & Innovation
Chris.white@secrc.co.uk | 07909 906177 |
www.linkedin.com/in/chriswhite3