



Nick Bell - Detective Superintendent

CEO - National Cyber Resilience Centre Group
National Policing Director - Cyber Resilience Centres
NPCC National Cybercrime Programme

NCRCG and Cyber Resilience Centres
2022

Cyber Resilience Centres - Threats and Challenges



2021 business population

- Est 5.6 million UK private sector businesses - SMEs account for 99.9%

Threats to business

- 4 in 10 businesses identified a cyber security breach or attack (DCMS Cyber Breaches 2021)
- 1.7m computer misuse crimes occurred over the year ending Dec 2020 (Crime Survey England and Wales 2020)
- A limited threat picture - Current under-reporting of cyber crime
- 2020/21 - 30,000 offences reported to Action Fraud (an annual increase of circa 20%)
- The UK's need for speed, ease, and access is increasing the need for technology
- Cyber crime identified as one of the biggest criminal threats to UK business and the economy

Challenges to SMEs

- Cyber security can be expensive
- Complexity in knowing how to protect your business
- Where do you go for help?

Cyber Threats



- **The return of Emotet malware and mass phishing campaigns for distribution**

Target: Global - Known to facilitate ransomware attacks, steal financial information and exploit victims in various ways.

- **Increased cyber threat due to the Russia-Ukraine invasion: DDoS, phishing, malware**

Target: Eastern Europe and Global – A rise in Distributed Denial of Service attacks by politically motivated groups, predominantly targeting critical organisations in support of either Russia or Ukraine.

New destructive malware and linked phishing attacks have also been observed.

- **Exploitation of zero day vulnerabilities: Follina heavily exploited**

Target: Global - The term “zero-day” indicates that there is no time between when a vulnerability is discovered by developers or researchers and when it is exploited by threat actors, making it a considerably dangerous attack vector.

Threat actors and nation state actors work quickly to exploit vulnerabilities with no fix, for example, a recent vulnerability dubbed ‘Follina’ affecting Microsoft Support Diagnostic Tool (MSDT) which could allow system takeover.



Cyber Threats



- **Increase in phishing emails with newer evasion techniques and the increased targeting of M365**

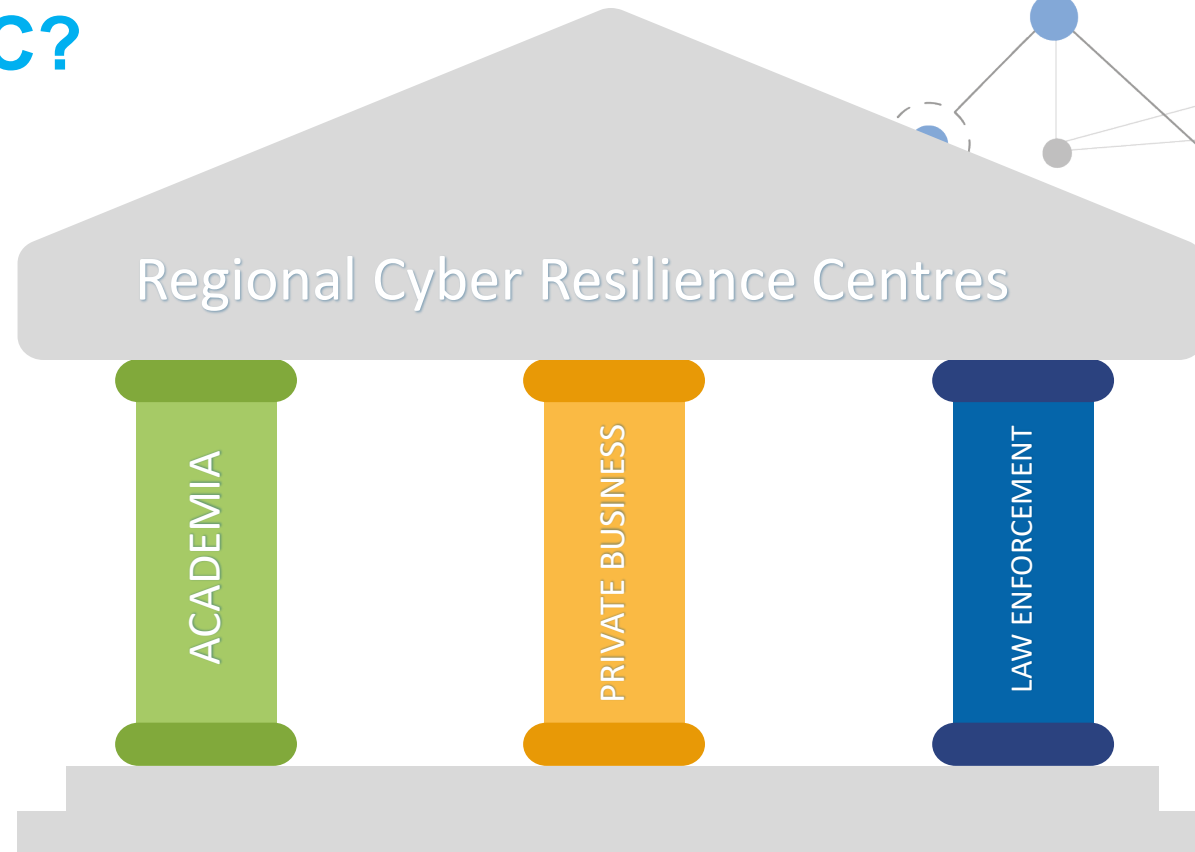
Target: Global - Threat actors are crafting increasingly sophisticated, highly convincing attacks that many people simply can't distinguish from legitimate actions. Microsoft 365 related attacks and phishing campaigns typically blend in with normal workday activities.

Techniques: customised URLs, spoofed email addresses, html attachments to evade detection

- **Ransomware groups consistently improve tactics, techniques and procedures (TTPs):**

Target: Global - Ransomware is increasingly improving its TTP's to gain a higher success rate, the latest technique includes deleting backups and shadow copies to prevent recovery of files.

What is a CRC?



Trust and Confidence

Who Are We Helping and Why?

Supporting the vulnerable and hardest to reach businesses

- SME + Micros who fall under the radar of the cyber security industry
- Businesses who may have never consumed a cyber security service
- Organisations with a low level of Cyber Resilience who only engage in response to an incident
- We look to introduce these organisations and businesses into the Cyber Industry through referral

Developing extensive reach through membership

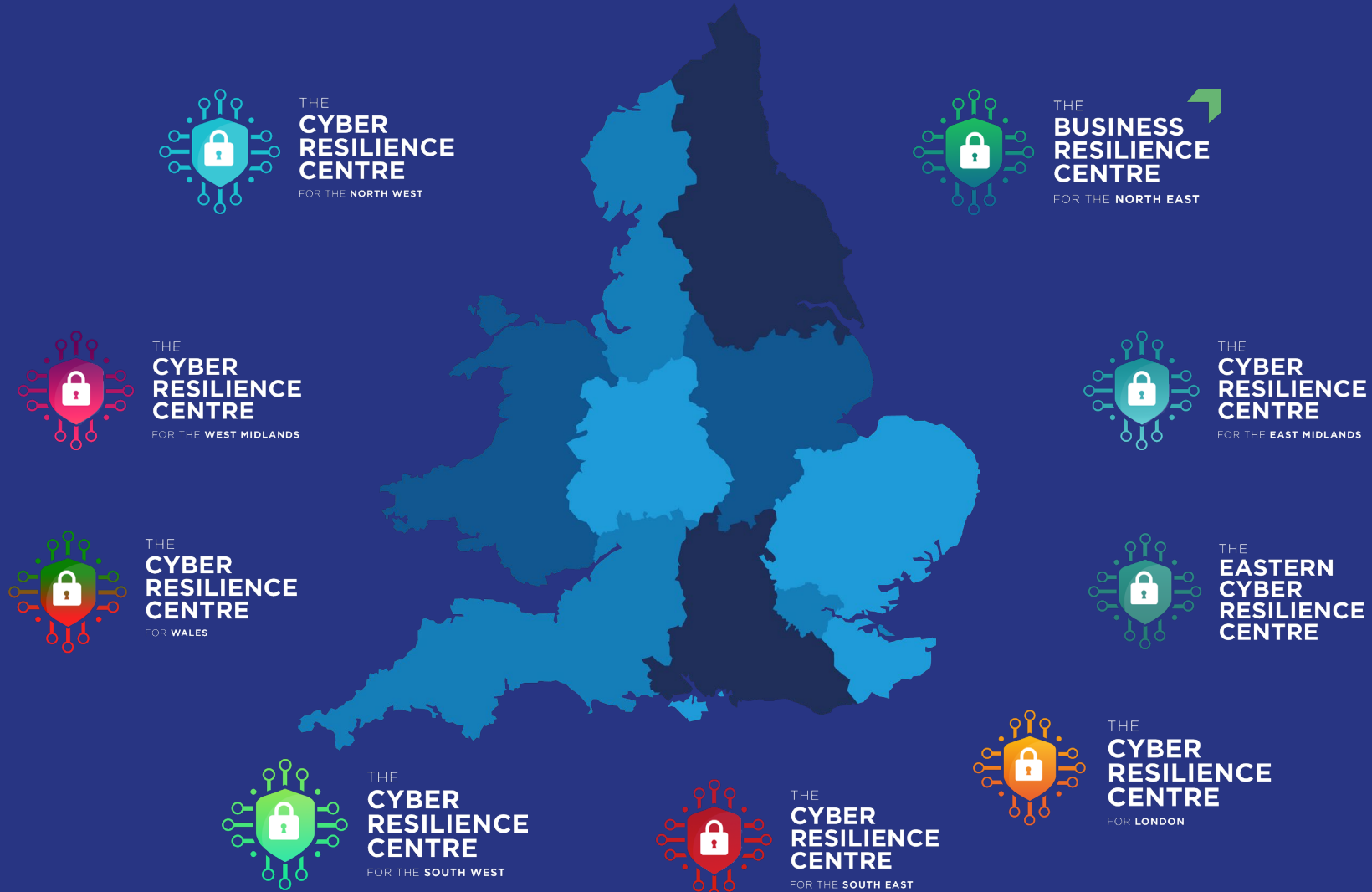
Offering affordable requirements led service delivery

- Augmenting the skills and experience of Cyber Students
- Providing real world experience & exposure into SME
- Offering a source of income during these challenging times

Every improvement we can make will raise the level of resilience



Regional CRC network





NATIONAL
**CYBER
RESILIENCE
CENTRE
GROUP**



To strengthen our national cyber resilience across Small & Medium-sized Enterprises (SMEs) through a police, private sector and academia not-for-profit partnership





Ministerial Launch

Thurs 09 December 2021 in York at the NEBRC annual reception.

The Security Minister RH Damian Hinds MP attends with Virginia Ayre from the Home Office and four Founding National Ambassadors from KPMG, CGI, Cantium Business Solutions and The Very Group.

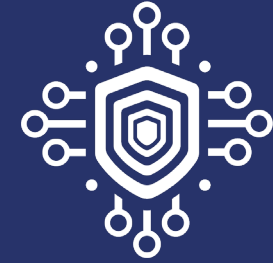


NATIONAL
CYBER
RESILIENCE
CENTRE
GROUP

Aims of the National CRC Group Ltd

- Strategically engage policing with the business community, collectively strengthening our delivery against the National Cyber Strategy
- Strengthen the Regional Cyber Resilience Centres, providing support to create a sustainable local model (whilst preserving their independence and regional strategies)
- Develop a National Student Services Programme pipeline that will deliver across all regions

National Student Services Programme



NATIONAL
CYBER
RESILIENCE
CENTRE
GROUP



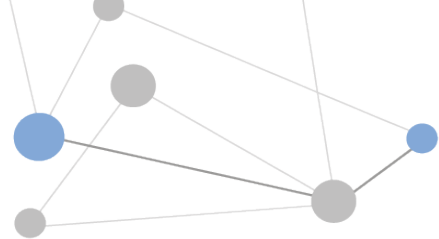
- Augmenting the skills and experience of Cyber Students
- Providing real world experience & exposure into SME
- Offering a source of income during these challenging times
- Developing a Cadre of Better Prepared Students
- Improving Cyber Resilience in the SME Community

The Why - A platform to lead the charge to strengthen our national cyber resilience and ultimately benefit the UK economy, protect our national assets, and make the UK a more attractive place to work, invest in and to deal with



The How - The better that we work together, harnessing the skills, knowledge and experience of police, government, large organisations and academia, the more resilient we can be as an entire economy





THE CYBER RESILIENCE CENTRE

Thank you for listening

Nick Bell CEO NCRCG

NPCC National Cybercrime Programme

nick.bell@nationalcrcgroup.co.uk



nick-bell-crc



NatPolDirCRC

