

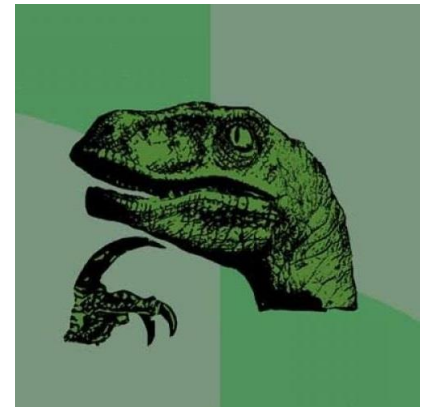


Department  
of Health &  
Social Care



# How can we improve Cyber Security Resilience across the NHS and social care?

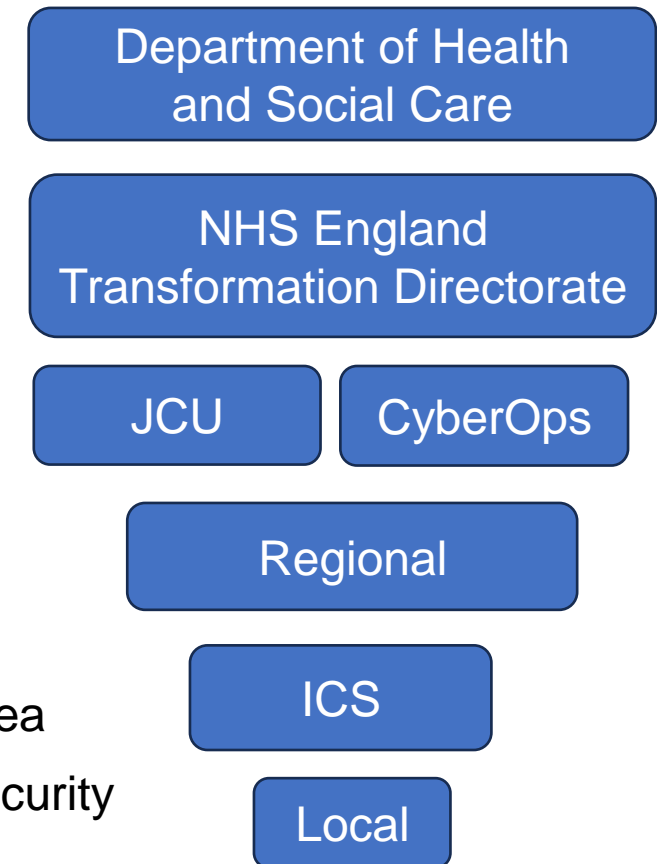
Paul Barnes, Head of Operations and Engagement – Cybersecurity  
NHS England Joint Cyber Unit, Digital Policy Unit





# Cyber Security in Health and Care - context

- A unified approach for a decentralised sector
- National cyber teams set direction and provide central support
- Supporting technical innovation and development and deployment
  - Economies of scale
  - Share learning
  - Ensure solid minimum level of security across the entire system
- Strategy, policy and standards. Manage systemic cyber risk
- Cyber Security Operations Centre
- Seven regional teams
- Integrated Care Systems (ICS) responsible cyber resilience across their area
- Health and social care organisations are responsible for their own cyber security



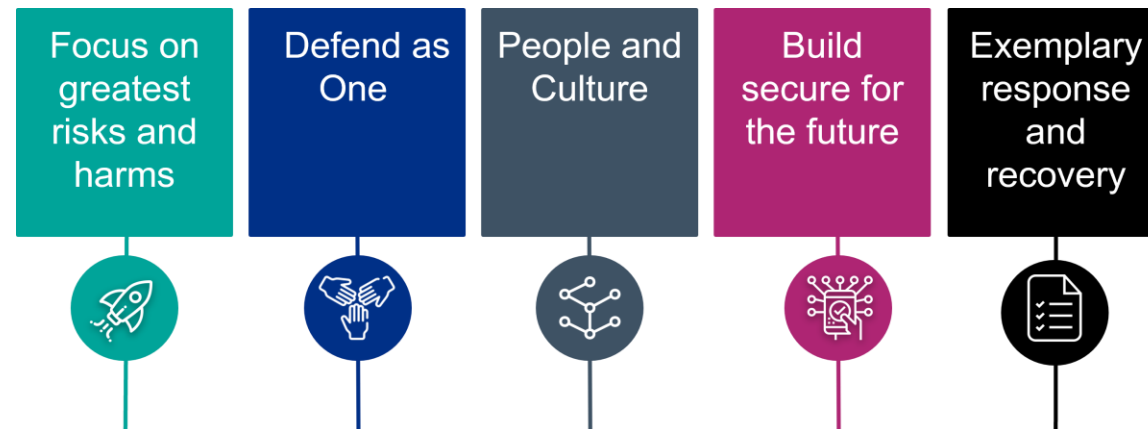


## Vision

A health and social care sector that is resilient to cyber-attack, in turn improving the safety of patients and service users.

## Approach

Five complementary pillars directing the system's overall approach to cyber resilience.





# Cyber Improvement Programme

- Our direct organisational scope includes almost **50,000 organisations**, made up of:
  - The NHS (primary/secondary/other);
  - Adult Social Care; and
  - Arms Lengths Bodies
- Deploying cyber security controls and building national and local capabilities
- Broadly the investment falls into three areas:
  - Developing security controls and capabilities
  - Targeted investment at ICS/provider level to reduce cyber risk and develop cyber capabilities
  - Expand the customer scope to reflect risk landscape.



# Cyber: Not just about tech

## Finance

Visibility of cyber spend across system

Investment proportionate to potential harm

Hospitals needing to replace unsupported systems - and budget needed for this

## Clinical

Understanding and articulating length of disruption and impact on patient care

Balancing dual risks of: patient harm and operational impacts of increased security controls/bureaucracy

Potential for patient harm when medical records are deleted by hackers.

## Workforce

Understanding, development, and promotion of cyber professionals

Recruitment, retention and re-entry policies for cyber workforce

Unable to recruit to cyber and digital roles (i.e. in ICBs/wider NHS) due to lack of talent

## Strategy and Operations

Consistency around local and national cyber strategies

Communicating security focus to increase trust and be clear on risks in innovations

Significant clinical, financial and reputational damage

## Commercial

Reflecting cyber standards in contracts – and enforcing

Understanding supply chain dependencies

Vulnerable suppliers being given NHS contracts (inc. access to data, pathways, etc)

## Tech

Implementing lifecycle management to prevent legacy tech

Balancing innovation and security

Cyber security policy *not* keeping pace with innovation e.g. AI, Apps



# 'Monumental' data breach exposes entire Northern Ireland police

By Christian Edwards and Jennifer Hauser, CNN  
Published 7:03 AM EDT, Wed August 9, 2023



Northern Ireland's Police Federation said the data breach is "potentially calamitous."

Technology

# Hackers who breached casino giants MGM, Caesars also hit 3 other firms, Okta says

By Zeba Siddiqui

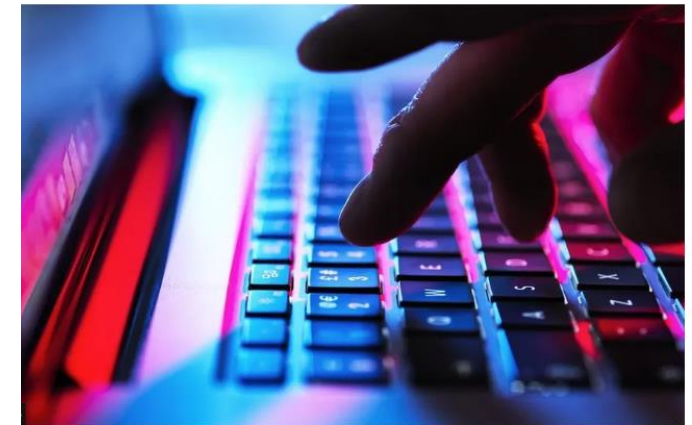
September 19, 2023 2:37 AM GMT+1 · Updated 8 hours ago



An exterior view of MGM Grand hotel and casino, after MGM Resorts shut down some computer systems due to a cyber attack in Las Vegas, Nevada, U.S., September 13, 2023. REUTERS/Bridget Bennett [Acquire Licensing Rights](#)

Irish Politics | Local News

# Massive data breaches across NI government departments



Information was left in a restaurant and there was possible disclosure of a former identity

Cracken

Information being left behind in a restaurant and the possible disclosure of a person's former identity are among serious government data breaches in Northern Ireland.





# MFA Policy

The policy currently applies to:

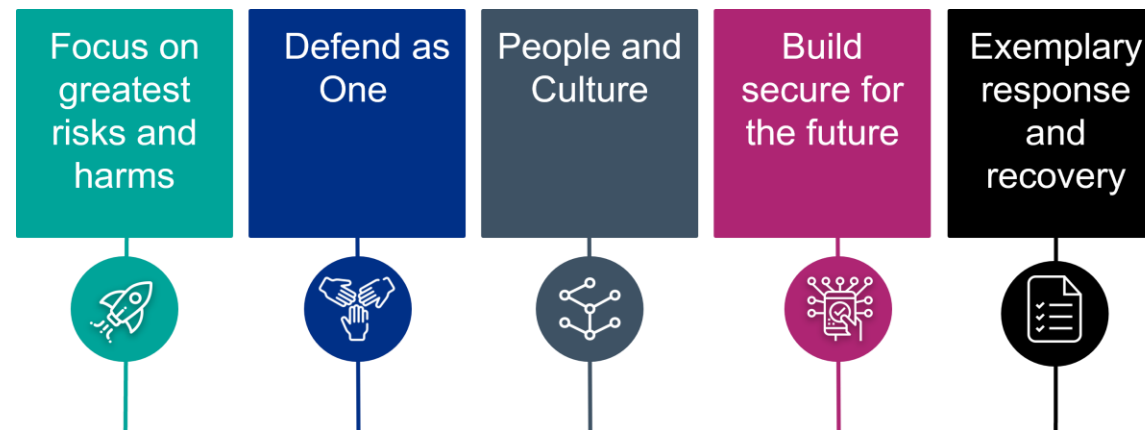
- NHS Trusts and Foundation Trusts
- Integrated care boards (ICB)
- Arm's length bodies of the Department of Health and Social Care
- Commissioning Support Units in NHS England
- Operators of Essential Services for the health sector in England





# What's next?

- Funding to Integrated Care Boards
- Strategy in a Box for Integrated Care Boards
- Supply chain and other partners
- Better Security Better Care
- Arm's Length Bodies

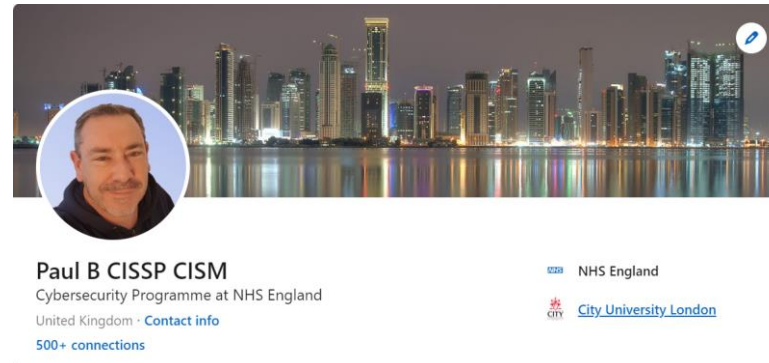






# Thank you

- **Cyber security strategy for health and social care: 2023 to 2030**  
<https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030>
- **MFA Policy**  
<https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy#:~:text=This%20policy%20will%20ensure%20that,have%20privileged%20access%20to%20systems.>
- **ISC2 “Certified in Cybersecurity”**  
One million free training courses and certification exam  
<https://www.isc2.org/certifications/cc>
- **Feel free to connect on LinkedIn**  
“Paul B CISSP CISM”  
<https://www.linkedin.com/in/pbarnes2>

**Paul B CISSP CISM**  
Cybersecurity Programme at NHS England  
United Kingdom · [Contact info](#)  
500+ connections

[NHS England](#)  
[City University London](#)



Department  
of Health &  
Social Care

