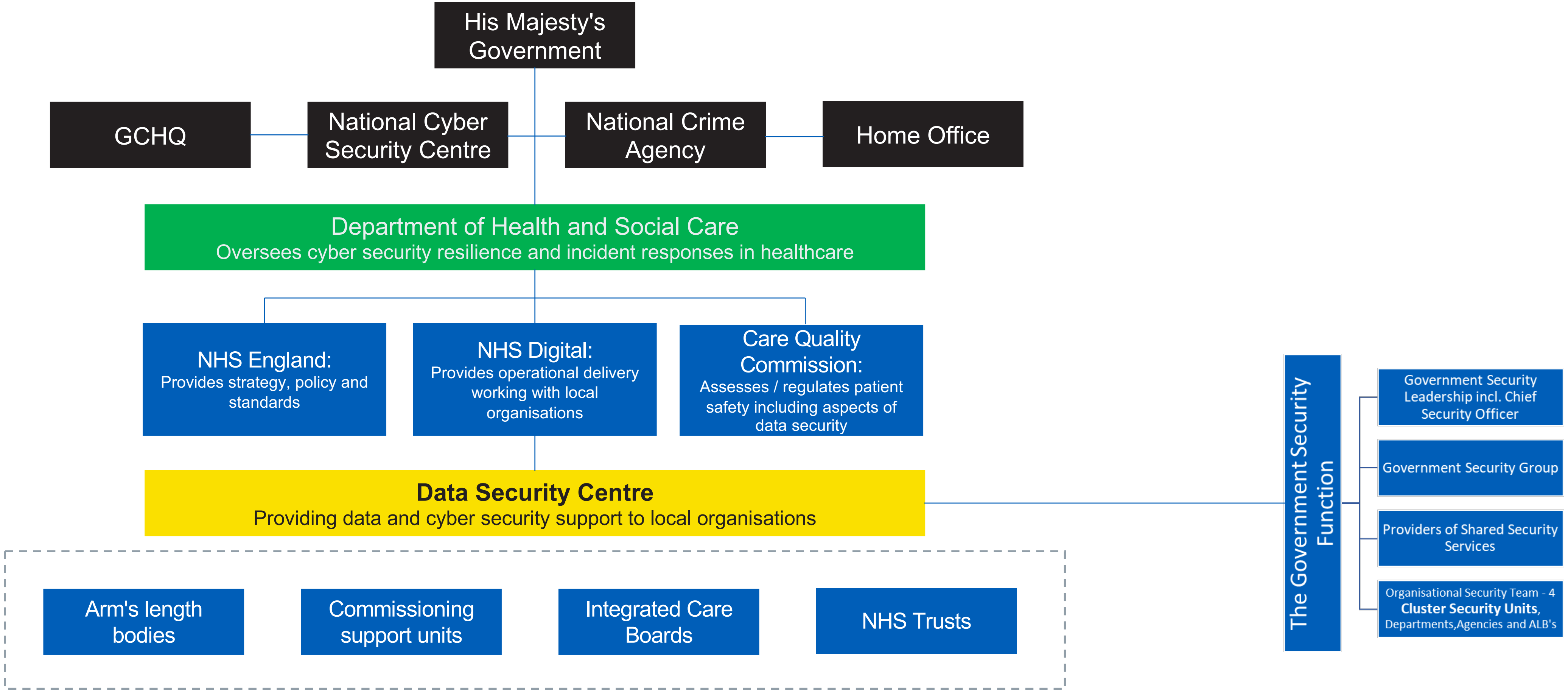
NHS
Digital

Cyber Security

What practices need to know and where to find support

Mark Logsdon, CISO NHS Digital

Where the Data Security Centre fits in



His Majesty's Government

GCHQ

National Cyber Security Centre

National Crime Agency

Home Office

Department of Health and Social Care
Oversees cyber security resilience and incident responses in healthcare

NHS England:
Provides strategy, policy and standards

NHS Digital:
Provides operational delivery working with local organisations

Care Quality Commission:
Assesses / regulates patient safety including aspects of data security

Data Security Centre
Providing data and cyber security support to local organisations

Arm's length bodies

Commissioning support units

Integrated Care Boards

NHS Trusts

The Government Security Function

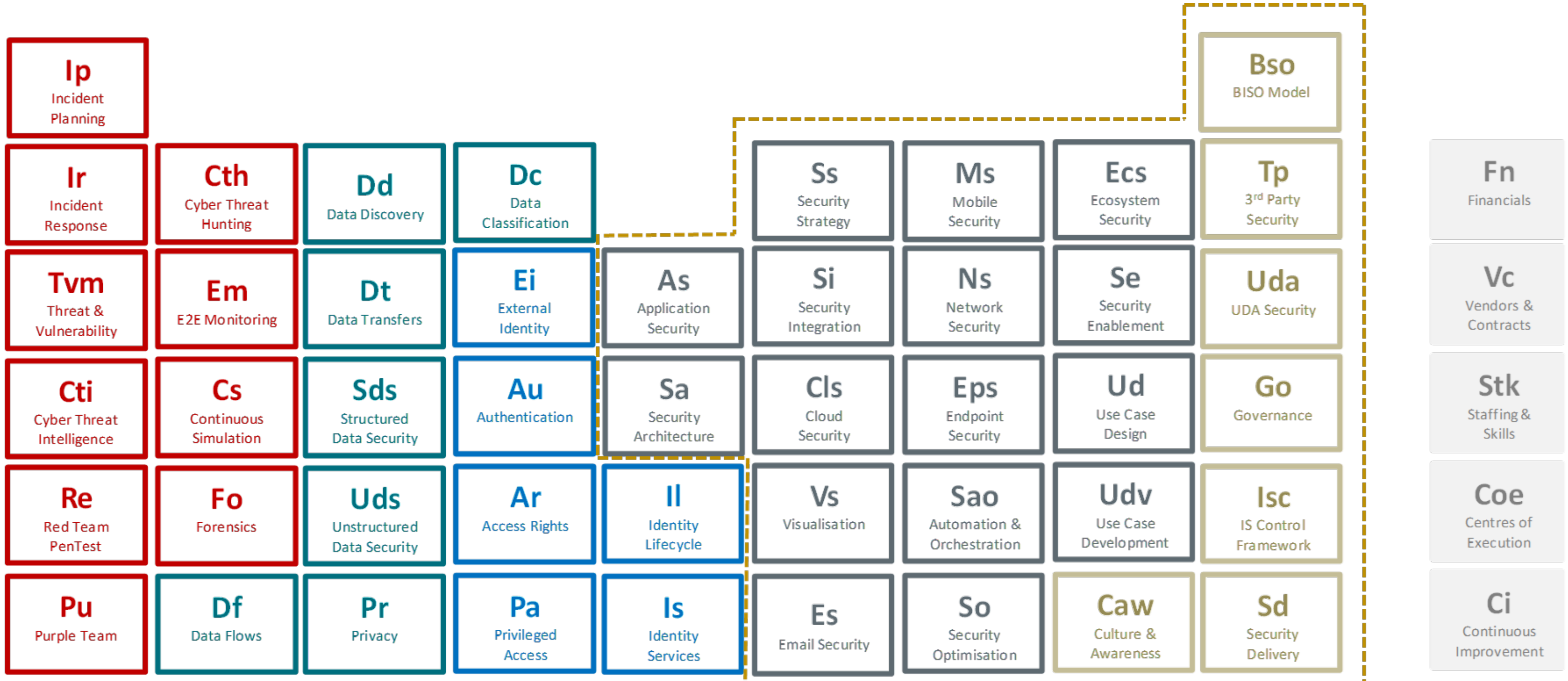
Government Security Leadership incl. Chief Security Officer

Government Security Group

Providers of Shared Security Services

Organisational Security Team - 4 **Cluster Security Units**, Departments,Agencies and ALB's

The Security Periodic Table – CISO Function



Ip Incident Planning								Bso BISO Model	
Ir Incident Response	Cth Cyber Threat Hunting	Dd Data Discovery	Dc Data Classification		Ss Security Strategy	Ms Mobile Security	Ecs Ecosystem Security	Tp 3rd Party Security	Fn Financials
Tvm Threat & Vulnerability	Em E2E Monitoring	Dt Data Transfers	Ei External Identity	As Application Security	Si Security Integration	Ns Network Security	Se Security Enablement	Uda UDA Security	Vc Vendors & Contracts
Cti Cyber Threat Intelligence	Cs Continuous Simulation	Sds Structured Data Security	Au Authentication	Sa Security Architecture	Cls Cloud Security	Eps Endpoint Security	Ud Use Case Design	Go Governance	Stk Staffing & Skills
Re Red Team PenTest	Fo Forensics	Uds Unstructured Data Security	Ar Access Rights	Il Identity Lifecycle	Vs Visualisation	Sao Automation & Orchestration	Udv Use Case Development	Isc IS Control Framework	Coe Centres of Execution
Pu Purple Team	Df Data Flows	Pr Privacy	Pa Privileged Access	Is Identity Services	Es Email Security	So Security Optimisation	Caw Culture & Awareness	Sd Security Delivery	Ci Continuous Improvement

Incident, Vulnerability & Threat Management
Identity & Access Management
Risk & Security Management

Privacy & Data Protection
Automation, Security Architecture & Services

NHS Security: Threats to the NHS

The NHS is considered a high value target for malicious cyber actors, including nation states and cyber criminals, because of the quantity and sensitivity of the information held about UK citizens, and the potential for criminal financial gain through fraud

Fraud	Data Theft & Espionage	Disruptive Cyber Attacks	Cyber Crime	Physical Crime	Protest & Campaign Activity	Country Security & Terrorism
Monitoring and detection	Vetting Data Loss Prevention	NHS Secure Boundary and MDE	Education Patching Encryption	Threat mgt Risk assessment Penetration testing	Preparedness Testing Industry Partnering	Cross Gov Security NCSC

Key Controls

- The NHS takes a holistic approach to managing security risk, ensuring that for Cyber, Physical, Personnel, Supplier Security and Business Continuity all attack vectors are considered together
- Unsupported and legacy systems are a security risk and could cause serious harm to patients
- NCSC provides detailed assessments of the key threat vectors to the NHS, specifically calling out ransomware, phishing, legacy unpatched systems, IT supply chain and cyber-enabled fraud as real and imminent threats to our business

What makes us a target?

92bn
Revenue

65 m
Health records

£92m
Disruption to services
(3 days Wannacry)

£££'s
Health record value

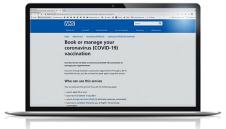
Supporting the frontline

Internal security

100

Security Champions

Across NHS Digital we have 100 security champions who are actively engaged. They act as ambassadors within their teams and regularly take part in security activities



Book or manage your coronavirus (COVID-19) vaccination

Use this service to book a coronavirus (COVID-19) vaccination or manage your appointments.

If you've already booked a vaccination appointment through a GP or local NHS service, you do not need to book again using this service.

Who can use this service

You can only use this service if any of the following apply:

- you're aged 25 or over
- you'll turn 25 before 1 July 2021
- you're at high risk from COVID-19 (clinically extremely vulnerable)
- you have a condition that puts you at higher risk (clinically vulnerable)

Data Security and Protection Toolkit

47k

submissions

Over 47,000 organisations submitted a DSPT return; the online self-assessment tool that allows organisations to measure their performance against the National Data Guardians standards

Incident volumes

300%

rise in cyber incidents

Since 2019 there has been a 300% rise in incident volumes; requirement to scale-up and increase automation

Cyber Associates Network

2200

CAN members

Over 2200 members of a peer to peer network aimed at improving cyber security across health and social care. Giving opportunities to discuss key issues in a safe space and learn from each other

High severity alerts

18

High severity alerts

A 60% increase on the previous year's high severity alerts. These are cyber security alerts that require immediate action to prevent damage to the network

Active defence

5m

transactions a week

We actively monitor and protect devices across the NHS and work directly with local teams in response to cyber threats

Security education

6k

downloads

Over 6000 downloads of security awareness materials from our Keep IT Confidential campaign. Topics include: social engineering, passwords, tailgating and be aware of what you share.

Devices protected

1.9m

devices enrolled

Devices enrolled onto Microsoft Defender for Endpoint which feeds directly into the cyber security operations centre enabling them to detect nefarious activity across the NHS network

Blocking malicious email activity

21m

malicious emails a month

On average CSOC blocks over 21 million emails every month. Working directly with local team to respond to the cyber threats

Protecting the NHS

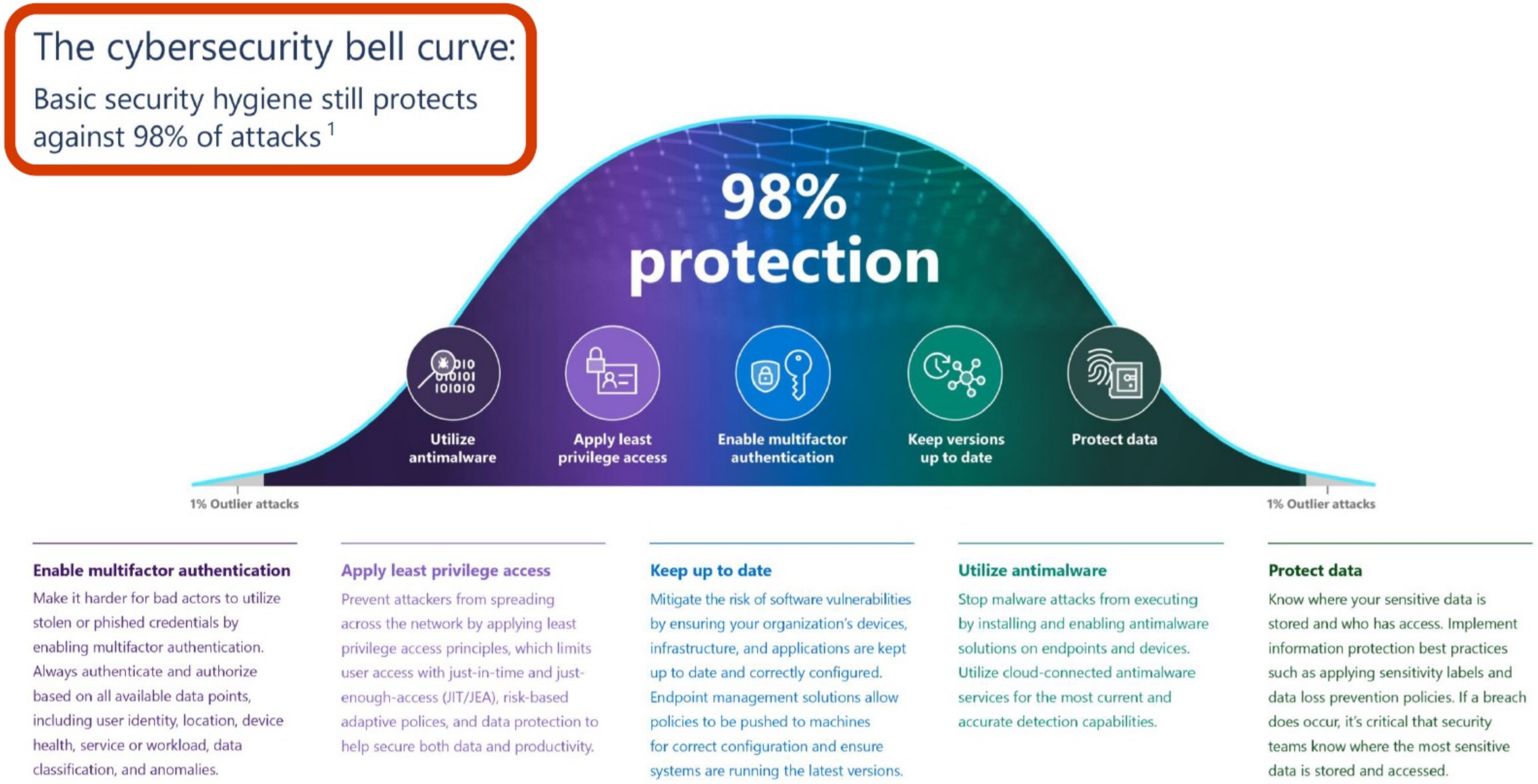
23.2bn

transactions

Protection of 23.2 billion transactions over a five day period through NHS Secure Boundary

Advice and help

5 Things to do today



The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks[1]

Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

Utilize antimalware

Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.

A word on Ransomware – top tips

Back ups

- Key data is frequently backed up
- Access is managed, multifactor authentication (MFA)
- Regular testing

Prevent malware delivery

- Mail filtering
- Malicious website blocking
- MFA for remote access

Prevent malware running

- Manage devices
- Anti-Malware
- Security updates
- Disable risky processes (e.g. macro’s, PowerShell)

Prepare

- Have a plan and test it
- Business continuity
- Agree communication lines to take
- Think about what your extortion response will be

The National Cyber Security Centre

National Cyber Security Centre

Background

The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber threats.

Since the NCSC was created in 2016 as part of the Government's five-year National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.

They support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public.

What NCSC can offer

Active Cyber Defence

Self service

- Web check
- Mail check
- Exercise in a box

Detections deployed by organisations

- Protective Domain Name Service (PDNS)
- Logging made easy
- Vulnerability disclosure

Disrupt threats

- Take down
- Suspicious email reporting

Standards and guidance

Cyber Essentials (CE) and CE+

an 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

Guidance

- Small Business Guide: Cyber Security
- Technical papers/advice
- Blogs
- “How to documents”

Find out more at https://www.ncsc.gov.uk/

The cyber associates network (CAN)

- A growing and engaging group
- Peer led – by members for members
- Over 2300 members made up of:
  - NHS Trusts
  - Integrated Care Boards
  - Arm’s Length Bodies
  - GP Practices
  - Local Government
  - Community Interest Communities

Find out how to join here

https://digital.nhs.uk/cyber

Advantage

❑ Shape and influence cyber security across health and social care

❑ Invitation to associate-only seminars and events

❑ Direct access to senior leaders and subject-matter experts

Innovation

❑ Advanced access to new and enhanced cyber security products

❑ Opportunities to pilot, test and develop DSC products, tools and services

Development

❑ Priority access to training opportunities; e-learning, wider professional development and accreditations

Improvement

❑ Direct support and guidance on how to improve cyber resilience within your organisation

❑ Feedback directly and candidly to the DSC on service improvement

Thank You

@nhsdigital

company/nhs-digital

digital.nhs.uk

NHS
Digital

Mark Logsdon
Mark.logsdon1@nhs.net