Data Security and NDG Review
Supporting the Wider System and National Data Guardian Review

Presented by Chris Flynn
Security Operations Lead
NHS Digital’s Data Security Centre
National Data Guardian Review
National Data Guardian Review

• NDG Review can be found here
• Published July 6th 2016
• Public Consultation through to September 2016
• Key Data Security Themes:
  – DH & its ALBs need to enable health and care to develop a better culture of data security
  – 10 Data Standards have been proposed as a minimum bar for health and care
  – Leadership and board level ownership is key to good data security
  – Leadership should own and be responsible for data security as they are for clinical and financial standards
NDG Leadership themes

Leadership Obligation 1: People
• Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Leadership Obligation 2: Process
• Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Leadership Obligation 3: technology
• Ensure technology is secure and up-to-date.
What are we protecting ourselves from?

Known threats and challenges in Health & Care
Potentially malicious activity

The NHS is no different to any other sector:

- Security threats commensurate to those found in wider industry are blocked at the gateway of the National NHS Network (N3) every month
  - That equates to malicious traffic equating to 0.3% of all data sent across the NHS Network
  - 276k downloaded files were quarantined suspected as being malicious—10% of these were blocked

- c.60% of incoming mails to NHS Mail2 were blocked as Spam
## Operating Systems across health & care

<table>
<thead>
<tr>
<th>Operating System</th>
<th>End of mainstream support</th>
<th>End of extended support/security updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>January 2015</td>
<td>January 2020</td>
</tr>
<tr>
<td>Windows XP</td>
<td>April 2009</td>
<td>April 2014</td>
</tr>
</tbody>
</table>

![Pie chart showing the distribution of operating systems across health & care](image)

- **Windows 7**: 83%
- **Windows XP**: 15%
- **Other**: 2%
The Threat is Real (& Health is no different)

**Hospital X:**
Infiltration onto local network; infiltrating 60+ internal servers (some clinical), used as a mail relay and over 2m SPAM emails sent from hospital servers. **Bedroom Hacker exploiting a Technology XP and Windows Server 2003 vulnerability.**

**Govt Body Y:**
Insider, an employee was socially engineered by a journalist to release pseudonymised information on hospital statistics that due to their format could have been re-ID’d. **Insider Threat, Social Engineering of Our People**

**Hospital Z:**
Malware attack, affecting 100 XP machines and multiple servers. Due to issues caused by data integrity fears, path results disrupted and discharge affected (bed blocking). **Criminality, failure in Process of the organisation to keep up their patching regime**
Balancing data security & patient care

Trust
Safe care
Timely care
Balancing data security & patient care

Confidentiality
Integrity
Availability

Trust
Safe care
Timely care
The Role of NHS Digital

And how they support the Data Security Standards
NHS Digital’s Data Security Centre is at the forefront of information and data security. It enables the secure and safe use of information within health and care building public trust through the services, guidance and advice it offers. It is the centre for threat intelligence while also coordinating a sector-wide incident management capability.

Capabilities:

- Cyber Security Programme delivering services to health and care
- Specialist Security Service – Internal specialists and resourcing
- Security Cell – internal security monitoring and incident management, external threat and incident management through CareCERT
NHS Digital’s Role in Data Security

NHS Digital’s Data Security Centre, the services it implements to health and care, and the support and guidance it offers to the system should be:

- non-regulatory; NHS Digital is not a regulator but an enabler to the 2million+ employees in the system to provide better data security
- a Leader in data security; the place the wider health and care system comes for advice guidance and support
- the gateway to the National Cyber Security Centre; distilling best practice and working with NCSC on improving UK response to cyber threat
- the trusted centre for threat intelligence for the system and sector wide incident management
Cyber Security Defence in Depth

- **People**
  - *Education & Training* e.g. Information Management Training Portal
  - *Personal Responsibility* e.g. CareCERT Knowledge
  - *Building a Security Culture* e.g. Data Security/IG Toolkit

- **Process**
  - *Defined Security Policies* e.g. CareCERT Assure
  - *Incident Management* e.g. CareCERT Intelligence
  - *Access Control* e.g. CareCERT Knowledge

- **Technology**
  - *Network Technology* e.g. N3 Gateview
  - *Patching and Encryption* e.g. CareCERT Intelligence & Cyber Capital Fund
Defence in Depth

Proactive

Data Security/IG Toolkit
CareCERT Assure
CareCERT Intelligence
Network Monitoring
CareCERT React
CareCERT Knowledge

Contractual Levers & Incentives

Information Management Training Portal
Cyber Capital Fund

Changing Culture
Removing Vulnerabilities
Blocking Threats
Reducing Impact
Continually Learning & Improving

Reactive

Proactive

Data Security/IG Toolkit
CareCERT Assure
CareCERT Intelligence
Network Monitoring
CareCERT React
CareCERT Knowledge

Contractual Levers & Incentives

Information Management Training Portal
Cyber Capital Fund

Changing Culture
Removing Vulnerabilities
Blocking Threats
Reducing Impact
Continually Learning & Improving
One More Thing… or four

Some final advice we give everyone across health and care:

- Data security needs to be about enablement!
- Invest in your people; personal responsibility in cyber is key.
- Don’t fall into the trap that Cyber Security doesn’t affect patient care or patient wellbeing, it does, and it is.
- Don’t entrust the security of the many with the few. We’re all on the hook to enhance what we do.
www.digital.nhs.uk
@nhsdigital
enquiries@nhsdigital.nhs.uk
0300 303 5678
CareCERT, React, Assure Enquiries:
cybersecurity@nhs.net