

digitalhealth

REWired

LONDON 14-15 MARCH 2023

Headline Sponsors:



SIMON NOEL

CNIO,
OXFORD UNIVERSITY HOSPITALS NHS
FOUNDATION TRUST



WHY CYBER SECURITY IS A PATIENT SAFETY ISSUE FOR ALL

WHAT IS THE ISSUE?

The number of digital trusts is growing

Digital is central to health strategy

Performance and oversight depends on reporting

Increasing use of independent systems

Oversight and governance vs clinical pressures

Recognition of the value/risks of data/digital

SOME RECENT ISSUES

Client data exfiltrated in Advanced NHS cyber attack

NHS ransomware attack spreads worldwide

Analysis

Killnet DDoS attacks inflicting damage on healthcare: 'This is war' with records left in 'chaos' three months on

back: what had is it?

Healthcare data breaches hit all-time high in 2021, impacting 45M people

COMPLIANCE & RISK

Ransomware attacks against healthcare organizations nearly doubled in 2021, report says

Healthcare Supply Chain Attacks Raise Cyber Security Alarm

Updated on January 11, 2023

EXAMPLES OF SOME CORE VULNERABILITIES

 Lots of data, data storage/locations

 Medical devices

 Increase in remote working

 Poor staff knowledge

 Complexity of the environment

 Requirement to share data

 Variety of organisations

 Legacy technology

WHAT ARE THE RISKS?

- Malware
- Password theft
- Traffic interception
- Phishing
- DDoS
- Cross site attack
- Zero day exploits
- SQL injection
- Social engineering
- MitM attack
- Cryptojacking
- Waterhole attack
- Drive-by attack
- Trojans



HOW DO WE
RESPOND?

10 STEPS (NCSC, 2022)

- Risk management
- Engagement and training
- Asset management
- Architecture and configuration
- Vulnerability management
- Identity and access management
- Data security
- Logging and monitoring
- Incident management
- Supply chain security



WHAT ARE THE KEY CLINICAL ISSUES?

- Clinical continuity
- Patient/service user safety
- Staff safety
- Research integrity
- Maintenance of trust/confidence

WHO IS VULNERABLE?



Hi Simon,

Throughout October 2022, we surveyed 600 UK CISOs and 2000 office workers to get some insight on how much visibility organisations have over their digital estates.

Many organisations are looking at how they can stay secure against the threats and challenges they'll face this year, such as:

- Cost control and consolidation challenges
- Digital transformation security challenges
- Increasing regulatory challenges
- New cyber challenges emerging from hybrid working
- Lack of skilled resources / cyber expertise and many more

I'm sending you an exclusive complimentary copy of the findings of our recent UK focussed cyber security peer group research.

More importantly, I'm including a list of strategies you can implement to overcome these issues.

[Click Here To Read Now](#)



WHAT DOES THIS MEAN DAY TO DAY?

Strategy

Investment

Governance

Oversight

Culture

Integration

WHERE DOES THIS FIT INTO STRATEGY?

Our

This

CyberSecurity Home
Report it
Training
Social engineering
Training
Phishing
COVID-19 Fraud Warning
Weak passwords
Tailgating
Unlocked screens
Meet the Team
Frequently Asked Questions
Document Library

Welcome to CyberSecurity



KEEP I.T. Confidential

Cyber security matters

Our Trust is moving rapidly towards its 'Paperless 2020' ambition and the way we care for patients is increasingly dependent on digital systems.

The use of internet, email, and more importantly the electronic patient record (EPR) has improved our efficiency as well as the quality of care we deliver. However for these systems to be effective we need to embed cyber security in our routine.

Good data and cyber security is our shared responsibility.

Everyone, including you, has a role to play in this for the safety of patients and staff.

Falling victim to cyber security attacks, including phishing (obtaining information fraudulently) and password theft will have a direct impact on our patients as well as on our work.

Better cyber security = improved patient safety

Cyber security is as important as infection control in ensuring patient safety and high quality care.

Hand-washing is something so routine to clinical staff that it is carried out as a matter of habit and viewed as an essential part of keeping people safe. We all need to routinely display the same levels of care towards cyber security, to keep our patients – and ourselves – safe.

There are some simple effective steps that everyone can take to maintain

I need to...

Choose task

Site managed by...

The list of members cannot be displayed because this site can be accessed by anonymous users.

Frequently Asked Questions

[View all FAQs](#)

objectives:

and wellbeing
passionate culture

s

lations.

nd will work together
le
nt appointments,

bate an inclusive culture

1 as our estates,

is research, education
act in improving

rovement

ulations.

Close to Home

Digital by Design



HOW DO WE INFLUENCE CULTURE?

- Needs to be built into planning
- Digital should be a baseline criteria
- Education and training should be central
 - WGLL
- Clinical and operational ownership

HOW DO WE SUPPORT OUR STAFF?

Training

Updating and
maintaining
equipment

Listen to the
challenges

Make
workarounds
redundant

Make it a
clinical issue

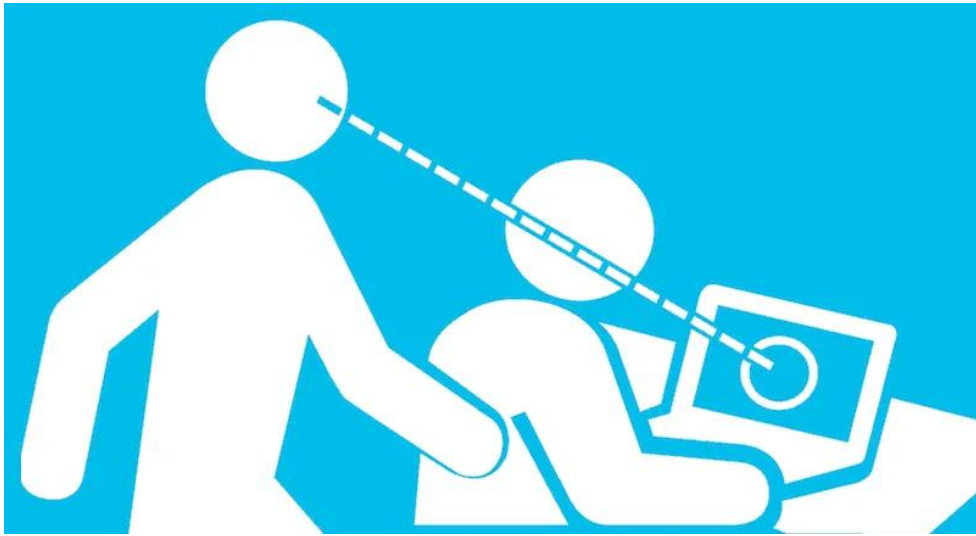
Be explicit
about data
accountability



ACCOUNTABILITY AND INSIGHT

- Dynamic and accessible environment
- Everyone has a “great idea”
- Who owns the output?
- What happens to the data?
- How is it supported
- Where is the governance?
- Clinical safety:
 - DCB 0129 & DCB 0160

WHAT ARE THE KEY MESSAGES?



- Cybersecurity is a clinical issue
- Operational planning is crucial
- Digital security from the ground up
- Support is key for ALL staff
- The tools, guidance and standards already exist

The background is a solid teal color with a subtle gradient. In the four corners, there are decorative white line-art elements resembling circuit traces or data paths, with small circles at the end of the lines.

THANK YOU

Any questions?