digitalhealth REWIRED LONDON 14-15 MARCH 2023

Headline Sponsors:

SystemC& Graphnet Care Alliance

tpp

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

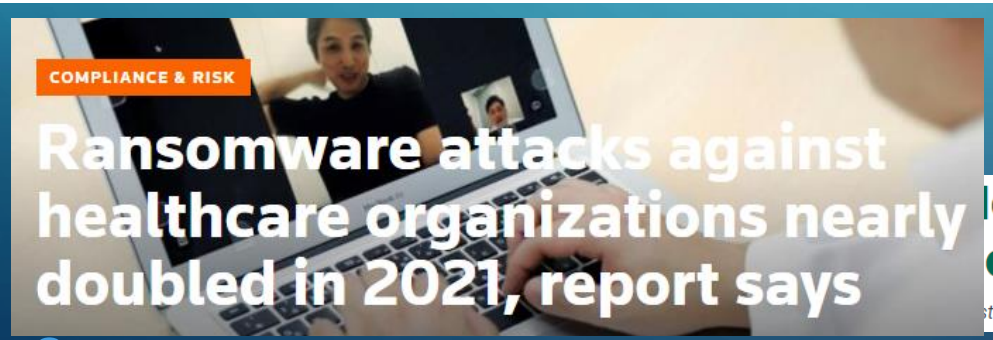
Analysis

Killnet DDoS attacks inflicting damage on healthcare: 'This is war'

ack: what
ad is it?

NHS cy
with records left in 'chaos' three months on

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



lealthcare Supply Chain Attacks Raise Cyber
ecurity Alarm

sted 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

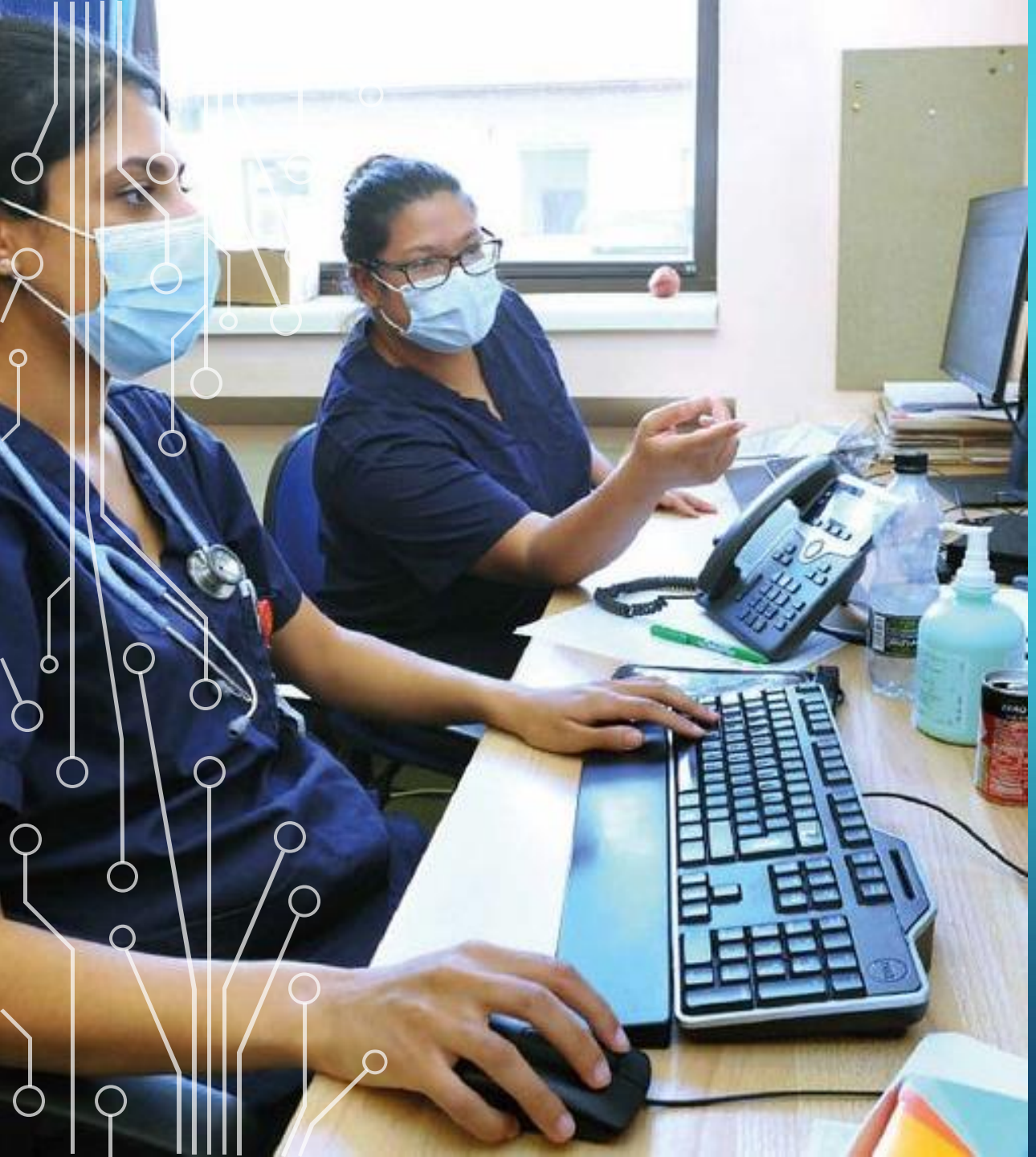
WHAT ARE THE RISKS?

- 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.

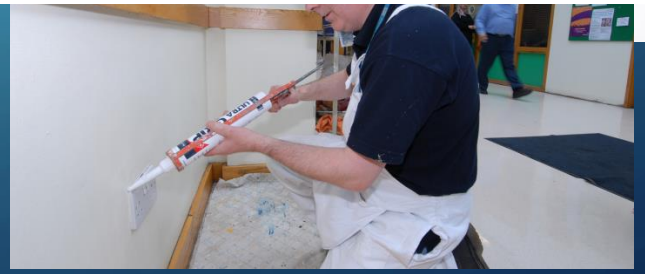
Many organisations are looking at how they can stay secure against the threats and challenges they'll face this year, such as:

- 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?

HOW DO WE INFLUENCE CULTURE?

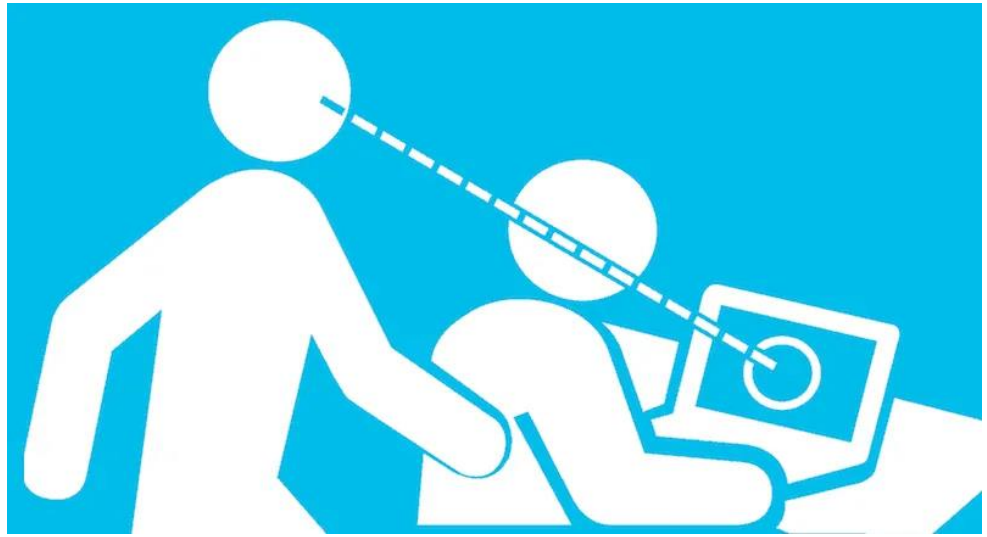
- Needs to be built into planning
- Digital should be a baseline criteria
- Education and training should be central
  - WGLL
- Clinical and operational ownership

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

THANK YOU

Any questions?