

Building Cyber Security Resilience Across the NHS

Paul Barnes, Head of Operations and Engagement - Cyber Security
16 September 2021



B
R
Pau
16 S

HS
ber Security

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:

 **12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw**



Where we started



- **This wasn't about Windows XP**
- **Most systems affected were unpatched Windows 7**
- **Resilience was there in the health and care system, but...**
- **Communications became a challenge as organisations disconnected from the network**
- **In the absence of a plan people made their own decisions**



Significant progress

Increasing our central ability to monitor and assure, but we need to go further

Cyber Security Operations Centre (**CSOC**), with oversight of the NHS desktop estate



Data Security Protection Toolkit (**DSPT**) - mandatory annual reporting against cyber standards



High Severity Alert (**HSA**) process, allowing us to track remediation to alerted vulnerabilities



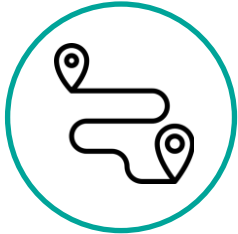
Regulatory powers over Trusts under Network and Information Systems (NIS) Regulations



Central offer of support, including firewalls, backup reviews, and bespoke technical remediation



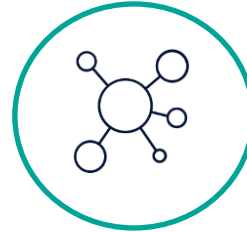
What we have done



**On-site
assessments**



**MS Defender for
Endpoint**



**NHS Secure
Boundary**



**Enhancement to
Cyber Security
Operations Centre**



**Response
metrics and
messaging**



**MS Office
licensing**



**Data Security
Protection
Toolkit**



**MS Windows
Licensing**

- **Roll-out of remote working at scale and pace**
- **Increased reliance upon technology**
- **Global rise in ransomware**
- **Importance of backups**
- **Massive datasets – Test and Trace / Mass Vaccinations**
- **Supply chain risks – SolarWinds “Sunburst”**
- **Health and care is no longer sacrosanct**

Recent cyber attacks on health



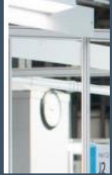
Coronavirus: Cyber-attacks hit hospital construction companies

© 13 May 2020



Cor

Prosecutors open homicide case after cyber-attack on German hospital



Incident in Düsseldorf could be first death caused by a cyber-attack, says

New Zealand hospital faces second week of disruption after major cyber attack



It is not clear what hospital, which



'Callous' ransomware attack has caused 'catastrophic' damage to Irish health care system

The attack has forced health workers to use paper records to keep services operational.



HSE Ireland
@HSELive



There is a significant ransomware attack on the HSE IT systems. We have taken the precaution of shutting down all our IT systems in order to protect them from this attack and to allow us fully assess the situation with our own security partners.

7:28 AM · May 14, 2021



1.6K 221 Share this Tweet

The threat landscape



Ransomware



**Hostile nation
state activity**



**Criminal cyber
groups**

- **Removal or reduction of unsupported systems**
Including versions of Windows 10 that are going out of date
- **Responding to High Severity Alerts when they are issued**
Ensuring systems are patched and up to date
- **Having in place robust, reliable, and immutable backups**
In line with National Cyber Security Centre guidance*

Strong cyber security is a non-negotiable part of transforming health and care.

Connect with us



NHSX Cyber team contact:
cybersecuritysupport@nhsx.nhs.uk

Paul Barnes
paul.barnes@nhsx.nhs.uk