

**SENT VIA EMAIL**

Email: [england.dt-pmomidlands@nhs.net](mailto:england.dt-pmomidlands@nhs.net)

16<sup>th</sup> April 2020

## **Re. Cyber Security and Covid-19**

Dear Colleague

The National Cyber Security Centre (NCSC) has assessed that COVID-19 presents an increased risk of a cyber-attack to healthcare services. Ransomware is a particular concern right now, it has been used already during COVID19 against healthcare in other countries and the criticality of the NHS right now makes it an attractive target to cyber criminals. Any type of cyber campaign could have a devastating impact on the NHS right now and therefore it is imperative that cyber security is strengthened across the entire NHS.

With this letter I include the official National Cyber Security Centre Report, 'How has COVID-19 changed the cyber threat to the health sector?'

To support organisations, NHSX has agreed a COVID19 Cyber Action Plan with NHS Digital and NCSC.

As part of that plan:

- NCSC is undertaking vulnerability scanning across the NHS. Where critical cyber vulnerabilities are found, they are being notified to NHS Digital and the relevant organisation. NCSC will recommend actions to be taken and suggest an appropriate time frame depending on the risk. Organisations should act quickly on these notifications and where needed NHS Digital will help or provide contractors to support you.
- NHSD is offering a range of centrally funded rapid technical remediation (boots on the ground) and where needed capital investment from NHSX to address critical cyber vulnerabilities. Using data available centrally this support is being targeted first at organisations most critical to the COVID19 response including the Nightingale Hospitals and those at greatest risk due to their cyber posture.
- Any organisations which may have unsafe back-ups in place are being immediately prioritised. This isn't about compliance and assurance, this is about the centre doing everything it can to try help your organisation be better protected as quickly as possible and paying for the work to happen. If your organisation is contacted over the next few weeks by NHS Digital, please do engage, contact in your region, is likely to come via Vicky Axon, your NHSD regional lead with NHSE/I regional leads kept informed.
- NHS Digital and NCSC have radically lowered the threshold at which they will intervene and if needed send in teams/contractors to help local organisations get back up and



running quickly in the event of an IT outage or cyber security incident. Please ensure your organisation reports any cyber incident at the first sign of trouble to **03003035222** (emergency helpline), or [carecert@nhsdigital.nhs.uk](mailto:carecert@nhsdigital.nhs.uk).

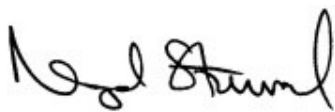
- Onboarding to NHS Secure Boundary for perimeter security will take your cyber security at organisational level an immediate big step forward. Contact your regional NHSD lead for more info and NHSX will fund firewalls where needed if this enables you to onboard more quickly.

**Any health organisation not maintaining good cyber hygiene is at risk. Some key questions leaders might want to ask within their organisations include:**

- Does our organisation have adequate back-ups in place, especially for our critical systems, to enable us to restore data quickly if we are hit by ransomware? Are back-ups stored correctly and regularly updated?
- Is our organisation up to date applying critical cyber security patches?
- Does our organisation operate any unsupported systems without other mitigations in place to protect them? If we have Windows 7, have we activated extended support on all the devices?
- Has our organisation rolled out Advanced Threat Protection as far as possible across the estate to take advantage of the additional protection it brings?
- Could we onboard quickly to NHS Secure Boundary? Weekly webinars available and access to funding to address infrastructure barriers.

If you would like any support please contact the Cyber Security mailbox at [cybersecurity@nhs.net](mailto:cybersecurity@nhs.net) or Victoria Axon, NHS Digital Regional Cyber Lead at [Victoria.axon1@nhs.net](mailto:Victoria.axon1@nhs.net) / 07712 693195.

Yours sincerely,



**Nigel Sturrock**

Medical Director & Chief Clinical Information Officer  
NHS England and NHS Improvement – Midlands

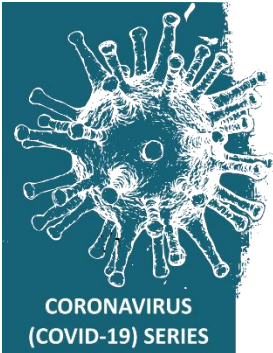
CC. Eddie Olla - Regional Director for Digital Transformation

# OFFICIAL

DO NOT UPLOAD THIS DOCUMENT TO ANY THIRD PARTY SERVICES. SEE HANDLING INSTRUCTIONS ON PAGE 4



National Cyber  
Security Centre  
a part of GCHQ



## How has COVID-19 changed the cyber threat to the health sector?

NCSC-A/R/1107-20

08 April 2020

### KEY JUDGEMENTS

- The UK health sector is **highly likely** now considered a high value target by a range of cyber actors. The COVID-19 pandemic has **almost certainly** increased the intent of cyber actors to target the sector.
- The largest threat to the health sector during the response to COVID-19 **highly likely** comes from cyber criminals deploying ransomware to take advantage of the disruption caused.
- Healthcare providers and organisations in the supply chain for medical equipment are **almost certainly** of increased interest to state actors seeking information to aid their own response to COVID-19.
- Members of the public and those working in the health sector are reliant on messaging being distributed by official websites; disruption of these websites is **likely**.
- The health sector will **highly likely** find maintaining high standards of cyber security increasingly challenging over the coming months.

### INTRODUCTION

1. The health sector is feeling the impact of COVID-19 more than any other Critical National Infrastructure (CNI) sector. It is the front line in the UK's response to the COVID-19 virus and many people's lives depend on its continued running.
2. The NHS has undertaken a major cyber security programme over the last two years, both nationally and locally. Every month they stop 21 million incidents of malicious activity on the national network and more than half a billion emails every three months.
3. The UK health sector comprises all NHS services provided by the NHS or private providers as well as social care. This paper also includes aspects of the sector's supply chain. For a full definition, see Annex A.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to [ncscinfoleg@ncsc.gov.uk](mailto:ncscinfoleg@ncsc.gov.uk). All material is UK Crown Copyright ©

OFFICIAL

# OFFICIAL

## WHAT ASSETS ARE AT RISK OF MALICIOUS CYBER ACTIVITY?

4. The general public are now reliant on technology for the dissemination of important information about symptoms and information on how to deal with the pandemic. Traffic to NHS websites would have almost certainly increased; disruption to this service through a Distributed Denial of Service attack (DDoS) will affect a range of people seeking trusted information and advice.
5. The NHS is relying on thousands of volunteers to provide certain services to those at serious risk from COVID-19. 750,000 people have now volunteered to assist the NHS as Volunteer Responders. The data of these volunteers, along with the data of over 1.5 million people deemed at serious risk, is necessarily held for the coordination and management of the services being provided. This data would likely be of interest to cyber actors to craft convincing spear-phishing emails for fraud or distribution of malware and to sell on to other criminals.
6. Vulnerabilities in Internet of Things (IoT) devices are well documented and it is well known that they are inherently insecure. These vulnerabilities can be exploited either through targeting the devices directly for disruption or using the device as an access point to the wider network. Cyber actors are already targeting medical devices<sup>1</sup>; however, the targeting of stand-alone devices on a hospital network is complex, and not all will necessarily connect to the internet. The complexity of targeting these devices compared with simpler attack methodology such as deploying ransomware makes it highly unlikely that this will be used against the health sector.
7. Hospital IT networks are almost certainly viable targets for cyber actors. Despite several cybercrime groups stating that they will not target organisations involved in the response to COVID-19, these groups do not speak for all cybercriminals, and there have already been hospitals and organisations involved in the pandemic targeted by ransomware. Any ransomware attack on NHS networks will likely disrupt the provision of healthcare. Paper backup systems will almost certainly be rolled out locally in place of those held on the network; however, lack of IT will highly likely disrupt information and data sharing between trusts and other authorities involved in the pandemic response.

## HOW WILL THE SECTOR BE TARGETED?

8. The health sector highly likely continues to be considered a high value target for a range of cyber actors. A range of attack methods, originating from different threat actors, will likely be used against the health sector during the period of response to COVID-19. It is unlikely that the health sector will be impacted by a large-scale cyber-attack such as WannaCry<sup>2</sup> or impacted by an attack on another CNI sector, similar to the NotPetya event<sup>3</sup>.

1 – In 2019, 11 models of insulin pumps were recalled over concerns that malicious actors could take control of the pump over a wireless connection and control the levels of insulin being administered. Additionally, in 2016, the US FDA issued a warning over vulnerable home monitoring systems for implanted defibrillators and in 2017 the same manufacturer recalled 465,000 pacemakers over similar vulnerabilities.

2 – WannaCry was a global cyber attack that shut down hundreds of thousands of computers around the world with messages demanding ransom payments. In the UK, it hit one third of hospital trusts and eight percent of GP practices. It cost the NHS £20 million between 12<sup>th</sup> May and 19<sup>th</sup> May and £72m in the subsequent clean-up and IT upgrades.

3 – NotPetya was a destructive attack masquerading as ransomware. It particularly affected Ukraine's financial and energy sectors, and government institutions, but spread further into Europe and Russia. The attack was conducted by inserting a malicious data encryption tool into a legitimate piece of software used by Ukraine's financial and government institutions.

# OFFICIAL

9. The greatest cybercrime threat to the health sector is highly likely from ransomware attacks. This is because criminals almost certainly believe that the pressure to pay a ransom will be increased during this period of heightened response. Ransomware, unless mitigated early, will likely disrupt an entire hospital or trust network, and restoring networks from backups could take a significant amount of time.
10. Healthcare providers and those in the supply chain, for example companies producing medical equipment and technology to aid the provision of care, are almost certainly of interest to state actors seeking information that could aid their own COVID-19 response and help them inform their foreign policy towards the UK during the pandemic. It is unlikely that this type of activity will cause disruption to the running of healthcare services. This type of attack will likely involve targeting employees with spear-phishing emails.
11. There have already been instances of website disruption against the health sector. This will likely continue and in most cases will unlikely be accompanied by any demands for payment. Cyber criminals and individuals motivated by mischief and ego are the most likely to conduct this type of attack. The anonymity of DDoS makes it extremely difficult to attribute attacks to a certain actor.
12. Since WannaCry, cyber security in the NHS has improved. IBM has been contracted to provide a Cyber Security Operations Centre, and Microsoft is providing up to date operating systems and their Advanced Threat Protection software. At a time of social distancing and working from home, those working in health sector cyber security will highly likely find it increasingly challenging to maintain the high level of security standards achieved since WannaCry. Members of staff working from home on personal devices also increases the risk that work accounts and health networks could be compromised. The increase in COVID-19 lures will likely make it harder for those working in the health sector to differentiate between genuine emails and malicious ones.

## ANNEX A – Definition of Health Sector

The following definition of the Health Sector is taken from NCSC-A/G/0005-18. In addition to this, the paper makes reference to the supply chain for medical devices and equipment.

There are four separate National Health Services operating in the UK: NHS England, NHS Scotland, NHS Wales, and Health and Social Care (HSC) in Northern Ireland – with some services provided on a cross-border basis. The UK health sector is comprised of all NHS services provided by the NHS or private providers as well as social care. This can be broken down into primary care including general practice, community pharmacy, dental and optometry services; non-primary care including acute trusts; as well as the social care sector including adult social care, residential care, and home care. The NHS in England holds the data for more than 65 million patients, employs approximately 1.5 million people, and deals with more than a million patients every 36 hours; this creates a huge amount of data that is important to the provision of care and needs to be accessible to a large number of devices and individuals, whilst also remaining secure.

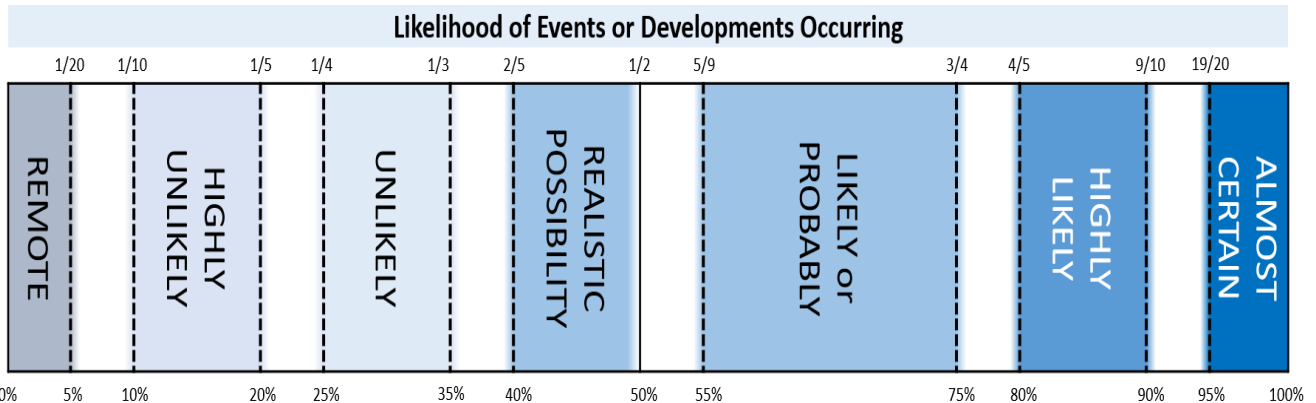
# OFFICIAL

## ASSESSMENT BASE

This report draws on industry reporting, open source information and government sources. There may be incidents conducted on behalf of state and non-state actors that have not been identified.

### Professional Head of Intelligence Assessment (PHIA) Probability Yardstick

NCSC Assessment uses the PHIA probability yardstick every time we make an assessment, judgement or prediction. The terms used correspond to the likelihood ranges below.



## CONTACT

For permission to quote or share this assessment or follow up questions or issues please contact NCSC Assessment Liaison.

Liaison: [liaison@ncsc.gov.uk](mailto:liaison@ncsc.gov.uk)

DD, NCSC-A: Eleanor F

## HANDLING INSTRUCTIONS

This report was issued at **OFFICIAL**.

Do not disseminate its content outside government channels without reference to the UK originator and ensure that appropriate need to know is enforced. Permission must be obtained from the originator for any further distribution outside your organisation or use of the information in summaries.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to [ncscinfoleg@ncsc.gov.uk](mailto:ncscinfoleg@ncsc.gov.uk).

Uploading this document to third party services without seeking permission is strictly prohibited.