NHS
St Helens and Knowsley
Teaching Hospitals
NHS Trust

Ref no:	218121120
From:	Public
Date:	12/11/20
Subject:	Cyber-attacks

REQUEST

A list of all cyber-attacks (both failed and successful) on NHS hospitals falling under your remit, in each year since 2015 (including broader cyber-attacks which include these hospitals). Where possible, please could you split the data as follows:

- Ideally, I am requesting **only** those cyber-attacks identified as or suspected of a) coming from a source within Russia or China; or b) emanating from any individual(s) or group(s) known to have, or suspected of having, links to the Russian or Chinese state. In each instance, please could you make clear which country the attack relates to.
- If this is not possible, please could you make clear whether an attack is thought to have come from inside/outside the UK.

In each instance, I am also requesting the following information:

- **The severity** of the attack, where it has been noted (e.g. low, medium, high).
- **The outcome** of successful attacks. For example: were documents stolen (and how many)? Was confidential data stolen (and how much)? Were any operations or other NHS processes cancelled or delayed as a result (and how many)?
- **The cost** to the NHS, where that cost is easily deductible/accessible. This could include but is not limited to a) delayed or cancelled operations, lost data, etc.; b) the security/staffing cost of defending against an attack; c) any consequent legal costs e.g. lawsuits filed successfully against the NHS as a result of personal data theft. If this part of the request is unduly onerous, please disregard.

RESPONSE

The Trust does hold this information, but considers it exempt under section 31 (1) (g) Law Enforcement, where disclosure would be likely to prejudice the exercise by St Helens and Knowsley Teaching Hospitals NHS Trust of its functions.

The Trust recognises that there is public interest in disclosure of information that increases transparency and demonstrates accountability within the NHS as to how cyber incidents may affect NHS Trusts. This has been taken into consideration when making this decision.

There is, however, a strong public interest in protecting confidentiality of patient data and ensuring that healthcare services can be provided to the public without increasing the possibility of attacks by hackers or malware, or putting personal or other information held on these systems at risk of corruption or subject to illegal access. Release of this information risks harming the systems the Trust relies upon on a daily basis.

As such, there is an overwhelming public interest in keeping the Trust's computer systems secure, which would be served by non-disclosure. For this reason the Trust has decided the public interest is to withhold this information.