St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	074230517
From:	Public
Date:	23/05/2017
Subject:	Wannacry Malware

REQUEST

Please provide the information below by return email:

1 What percentage of the Trust's Microsoft Windows machines (servers, PCs, laptops) was affected, locked or otherwise knocked-offline by the WannaCry ransomware attack?
2 Please provide the total number of machines affected.
3 Of this total number, how many were Windows XP machines?
4 How long were the affected machines rendered unusable in terms of hours or days?
5 What steps did the Trust take to recover the affected machines?
6 Which applications or services at the Trust were directly affected as a result of the attack?
7 How many times did your Trust pay the ransom demanded by the WannaCry malware to unlock any of the affected machines?
8 What data was lost from the Trust as a result of the WannaCry attack?
9 Since your WannaCry attack, what new security technologies has the Trust deployed to ensure the future integrity and safety of its Windows IT systems?

If it is not possible to provide the information requested due to the information exceeding the cost of compliance limits identified in Section 12, please provide advice and assistance, under your Section 16 obligations, as to how I can refine my request to be included in the scope of the Act.

RESPONSE

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information above would highlight any vulnerability, should any such vulnerability exist (within hardware or software or architecture or Vendor, etc.), within our IT infrastructure which could be exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust.

This information relating to the cyber security agenda is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

Our patients (and staff) must have confidence that their very sensitive personal data will be held securely.

They (patients & staff) must have confidence that we'll be able to provide the services they need.

Therefore, providing the specific requested information would put their confidence at risk.

Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

And therefore, this would be extremely harmful to the public & the services the Trust provides.

Therefore in accordance with Section 31 of the Freedom of Information Act the Trust will not be releasing the requested information as this would prejudice our ability to resist cyber-attacks.