

Ref no: 105140617
From: Press
Date: 14/06/17
Subject: Infected computers

REQUEST

1. How many computers in your Trust were infected with ransomware in the WannaCry attack in May this year?
2. How many (i) operations and (ii) patient appointments were cancelled as a result of the WannaCry attack?
3. How much money did you pay to enable you to use these computers again following the WannaCry attack?
4. In (i) 2014/15 and (ii) 2015/16 how many times were the Trust hit by ransomware attacks and how much money did the Trust pay to the cyber criminals to release your machines?

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.