St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	725150317
From:	Commercial
Date:	15/03/17
Subject:	Cyber attacks

REQUEST & RESPONSE

If this request is too wide or unclear, I would be grateful if you could contact me as I understand that under the Act, you are required to advise and assist requesters. If any of this information is already in the public domain, please can you direct me to it, with page references and URLs if necessary?

I understand that you are required to respond to my request within the 20 working days after you receive this letter.

1. Has your organisation completed all of the government's '10 steps to cyber security'?
   - ○ Yes – **Always working towards and improving**
   - ~~○ No~~

2. Have you suffered Distributed Denial of Service (DDoS) cyber attacks on your network in the last year?
   - ~~○ Yes~~
   - ○ No

3. If so, how many DDoS attacks did you experience during 2016? **N/A**
   a. Attacks occur weekly or even daily
   b. Attacks occur monthly
   c. Less than a handful of attacks during the entire year

4. Has your organisation ever been the victim of a DDoS attack which was used in combination with another type of cyber attack, such as a demand for ransom/ransomware, network infiltration or data theft?

- ~~Yes~~
- No

5. How does your IT team detect that your organisation has suffered a DDoS attack?
   - ~~End-users complain of a service issue~~
   - High bandwidth spikes with other network security tools
   - ~~Infrastructure outages/failures, (e.g. firewalls went down)~~
   - ~~Application failures, eg. Websites going down~~

6. Does your method of DDoS mitigation detect sub-saturating DDoS attacks of less than 30 minutes in duration, which do not typically overwhelm the network? **See below**
   - Yes
   - No

RESPONSE

See above 1 to 5 and for 6:

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. Therefore, to confirm or deny such architecture in our IT network 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.

Again, providing information about applications we use or parameter settings and aid to the foot printing phenomena.

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.