Ref no:	500081116
From:	Press
Date:	08/11/16
Subject:	Cyber attacks

REQUEST

1. How many times has your organisation been a victim of a cyber attack in the last two years?

2. How many times has your organisation been a victim of a ransomware attack in the last two years? In each case, was a ransom paid and if so how much was paid?

3. For each of the cyber and ransomware attacks, please provide a summary of the incident. This should including details of who was targeted, how they were targeted, what the immediate impact was, for instance was patient or staff data targeted, and if so in what way and how many people's data was affected? For each of the attacks, please also detail whether the police became involved, and whether the perpetrator or perpetrators were caught?

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 would highlight any vulnerability, should any such vulnerability exist, 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 vulnerabilities in our IT network is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust.

Therefore: To confirm or deny whether or not our organisation been a victim of a cyber-attack would motivate attacks against our network which would massively hinder our abilities to safeguard the service user healthcare Information and staff information that we require to coordinate our services.