

<b>File reference</b>	W17FOI280
<b>Key words</b>	Cybercrime
<b>Date of release</b>	11/06/2017
<b>Attachments</b>	No

## **Freedom of Information Act Disclosure log - Reply Extract**

**You asked these questions in five separate emails sent on the same day**

### **Email one**

**Under an above request could I please ask how many computers across your trust use windows xp?**

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply.

### **Email two**

**Under an above request could I enquire what the predicted/estimated cost to your trust is/for/against cyber attacks across 2017 ?  
Additionally what has/is the current cost to date ?**

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply.

### **Email three**

**Under an above request could I please ask how many patients had to be notified of an appointment being cancelled due to the cyber attack on NHS Systems on the 12th of may 2017?**

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply.

### **Email four**

**Under an above request could you advise how many attempted Cyber attacks have been directed at your trust in 2016 and 2017 to date ?**

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply.

## **Email five**

### **How many computer infection attempts have been cleared/stopped by your firewall or antivirus software by day for the month of may 2017 so far?**

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply to the questions you have asked.

## **Our legal statement relating to the use of exemptions**

### **Introduction**

Section 31 and 38 apply to all of the questions you have asked. We are sorry that we cannot be more helpful, but trust that you will understand our approach in light of the risks associated with responding, particularly in light of recent national news events about cybercrime.

We have for some time adopted a similar approach to all requests about our integrated network security and believe this is necessary in maintaining the highest levels of security.

### **Exemptions applied**

Section 31.-(1) (a) the prevention or detection of crime applies, as does 31.-(3) neither confirming nor denying we hold the information requested.

Section 38-(1) (a) and (b) the Health and Safety exemption applies. Additionally section 38.-(2) applies in that we are neither confirming nor denying we hold the information requested.

## **Exemptions use rationale**

This disclosure would prejudice the prevention and detection of crime and any information, albeit confirming what we hold or do not hold could assist criminals and place our patients and staff at harm. The Trust has provided a more detailed rationale below for each exemption used and applied them following the careful consideration of submissions made to a Public Interest Test in deciding the outcome of our response to you.

### **Section 31 – Law enforcement- prevention of crime**

We consider this exemption applies because disclosing details of our security arrangements could prejudice the security and integrity of the Trust's network and increase the risk of unauthorised access to information held by the Trust, much of which is confidential and sensitive. The level of detail that would be released would enable external parties, who are not privy to the confidential aspects of Trust's IT systems, knowledge of our security equipment and by association its integrated network security. The Trust employs a range of security tools to mitigate the risk from different types of security threats. Firewalls, Intruder Detection Devices Antivirus and other products form a mesh of security that protects the Plymouth NHS Network and data, the more of these vectors that are known, the weaker the security of the network protection. There is a real risk that this knowledge could assist external parties in attempting a cyber-attack/hack into the Plymouth NHS Network. The anticipated harm from this is a breach of data protection (failure to protect information resulting in an unauthorised disclosure), data loss, and disruption to patient care through a loss of IT services. The severity of harm is extensive with millions of patient records put at risk of unauthorised disclosure.

### **Section 38 Health and Safety**

Such disclosures also endanger the physical or mental health and safety of patients and staff. The dangers have become self-evident from recent events reported in the news, including delays to treatment and diagnostics to name but a few. Any failure of our infrastructure endangers both the physical and mental health of our patients and exposes them to danger.

**Attachments included:** No