File reference	W17FOI277
Key words	Cybercrime
Date of release	12/06/2017
Attachments	No

Freedom of Information Act Disclosure log - Reply Extract

You asked

I'm writing with a series of requests for information relating to the recent ransomware incident affecting you, this information is requested as it was at the time of this attack (except for logs which by nature will show before and after).

For all desktop, laptop and server computers in use by you please provide the following information (if you anticipate this information being difficult to collate for your entire network then please limit it to machines affected by this ransomware):

1. **What operating system was in use including what version, release version, service pack/build etc (e.g. Windows XP Service Pack 3 build 2600 release NT 5.1)?**
2. **Is the OS currently supported e.g. for updates? Is this through a standard licence (e.g. windows 10) or a bespoke contract (e.g. continued support agreement for Windows XP)?**
3. **For the affected machines (or for all machines in the same category if this is done centrally and deployed to the individual machines wholesale), along with your relevant servers etc, could you please provide the following information:**
4. **Please provide the full relevant update history/histories log where available (this may provide helpful guidance https://support.microsoft.com/en-gb/help/902093/how-to-read-the-windowsupdate.log-file). This may be held centrally or PC by PC.- Specifically, even if for any reason you do not provide the full log as requested or alongside it, could you say 1. When was the last system update and /or security patch installed?, 2. has the MS17-010 patch been installed on the machine/s and 3. has/have the machine/s had Microsoft's full March 14 'patch Tuesday' patch releases installed?**

Our reply

Beyond the information published on the Trust's website, we are not able to provide further information. The Trust cannot provide answers to your questions because exemptions apply. Please refer to our legal statement below.

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.