Maidstone and
Tunbridge Wells
NHS Trust

Ref: FOI/GS/ID 7089

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net
www.mtw.nhs.uk

01 December 2021

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Information Technology.

You asked:
1. Do you have a formal IT security strategy? (Please provide a link to the strategy)
A) Yes
B) No
2. Does this strategy specifically address the monitoring of network attached device configurations to identify any malicious or non-malicious change to the device configuration?
A) Yes
B) No
C) Don't know
3. If yes to Question 2, how do you manage this identification process – is it:
A) Totally automated – all configuration changes are identified and flagged without manual intervention.
B) Semi-automated – it's a mixture of manual processes and tools that help track and identify configuration changes.
C) Mainly manual – most elements of the identification of configuration changes are manual.
4. Have you ever encountered a situation where user services have been disrupted due to an accidental/non malicious change that had been made to a device configuration?
A) Yes
B) No
C) Don't know
5. If a piece of malware was maliciously uploaded to a device on your network, how quickly do you think it would be identified and isolated?

A) Immediately
B) Within days
C) Within weeks
D) Not sure
6. How many devices do you have attached to your network that require monitoring?
A) Physical Servers: record number
B) PC's & Notebooks: record number
7. Have you ever discovered devices attached to the network that you weren't previously aware of?
A) Yes
B) No
If yes, how do you manage this identification process – is it:
A) Totally automated – all device configuration changes are identified and flagged without manual intervention.
B) Semi-automated – it's a mixture of manual processes and tools that help track and identify unplanned device configuration changes.
C) Mainly manual – most elements of the identification of unexpected device configuration changes are manual.
8. How many physical devices (IP's) do you have attached to your network that require monitoring for configuration vulnerabilities?
Record Number:
9. Have you suffered any external security attacks that have used malware on a network attached device to help breach your security measures?
A) Never
B) Not in the last 1-12 months
C) Not in the last 12-36 months
10. Have you ever experienced service disruption to users due to an accidental, non-malicious change being made to device configurations?
A) Never
B) Not in the last 1-12 months
C) Not in the last 12-36 months
11. When a scheduled audit takes place for the likes of PSN or Cyber Essentials, how likely are you to get significant numbers of audit fails relating to the status of the IT infrastructure?
A) Never
B) Occasionally
C) Frequently
D) Always

Trust response:
The Trust is applying Section 31(3) in response to the request.
S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.
As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

The NHS Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the NHS Trust’s ICT infrastructure and would reveal details about the Trust’s information security systems. The NHS Trust recognises that answering the request would promote openness and transparency with regards to the NHS Trust’s ICT security.