University Hospitals Bristol and Weston NHS Foundation Trust

Freedom of Information Request Ref: 21-616

10 December 2021

By Email

Dear Sir/Madam

Thank you for your request for information under the Freedom of Information Act 2000. The Trust's response is as follows:

- We can confirm that we do hold the information you are requesting

1. Do you have a formal IT security strategy? (Please provide a link to the strategy)
A) Yes

B) No – Currently being written in conjunction with Exec lead.

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– Currently being written in conjunction with Exec lead.

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.
Not applicable

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 –

University Hospital Bristol and Weston NHS Foundation Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here: http://www.legislation.gov.uk/ukpga/2000/36/section/31

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.
Factors in favour of confirming or denying the information is held
The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the Trust's digital infrastructure and would reveal details about the Trust's information security systems. The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's digital security.
Factors in favour of neither confirming nor denying the information is held
Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.
In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.
Balancing the public interest factors
The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extend the Trust is able to detect and deal with digital security attacks. The Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's digital systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other

similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's digital systems.

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
See response to question 4 above

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
See response to question 4 above

7. Have you ever discovered devices attached to the network that you weren't previously aware of?
A) Yes

B) No
See response to question 4 above

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.
Not applicable

8. How many physical devices (IP's) do you have attached to your network that require monitoring for configuration vulnerabilities?
Record Number:
See response to question 4 above

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
See response to question 4 above

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
Not in the last 1-12 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
See response to question 4 above

This concludes our response. We trust that you find this helpful, but please do not hesitate to contact us directly if we can be of any further assistance.

If, after that, you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to:

Director of Corporate Governance

University Hospitals Bristol and Weston NHS Foundation Trust
Trust Headquarters
Marlborough Street
Bristol
BS1 3NU

Please remember to quote the reference number above in any future communications.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Publication

Please note that this letter and the information included/attached will be published on our website as part of the Trust's Freedom of Information Publication Log. This is because information disclosed in accordance with the Freedom of Information Act is disclosed to the public, not just to the individual making the request. We will remove any personal information (such as your name, email and so on) from any information we make public to protect your personal information.

To view the Freedom of Information Act in full please click here.

Yours sincerely

Freedom of Information Team
University Hospitals Bristol and Weston NHS Foundation Trust