NHS Borders
Communications & Engagement

NHS Borders
Education Centre
Borders General Hospital
Melrose
Roxburghshire
TD6 9BD
01896 825545
foi.enquiries@borders.scot.nhs.uk

Freedom of Information request 28-23

Request

1. What was the total number of cyber-attack incidents that have been recorded in your trust in the past 24 months?

2. What is the classification of your policy regarding breach response?

3. Of the devices running Windows operating systems, what is the number and percentage of devices running Windows 11, Windows 10, Windows 7, Windows XP?

4. What are the top 20 cyber security risks in your Trust, and how are they managed?

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified / managed.

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?

7. What is your current status on unpatched Operating Systems?

8. Of the devices running Windows Servers operating systems, what is the number and percentage of devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019, Windows 2022?

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?

10. Does your Trust hold a cyber insurance policy? If so:

    a. What is the name of the provider;
    b. How much does the service cost; and
    c. By how much has the price of the service increased year-to-year over the last three years?

11. When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals?

12. Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection?

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?

14. How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants?

15. Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?

16. How much money is spent by your Trust per year on public relations related to cyber-attacks? What percentage of your overall budget does this amount to?

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?

19. What is your strategy to ensure security in cloud computing?

20. Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System / Application, and the total spend for enhanced support?

Response

1. NHS Borders has recorded 1 Cyber related incident in the last 24 months.

2. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

3. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

4. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

5. The Unified Cyber Risk Framework is not used within NHS Scotland.

6. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

7. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

8. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

9. The NHS Secure Boundary is not used within NHS Scotland.

10. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

11. Cyber Security is reported into the Information Governance committee with half yearly updates to the board Audit Committee. The Executive Team took part in a Cyber Training Exercise in July 2022. Our Senior Information Risk Owner (SIRO) has completed board / director training which was provided by Cyber Security Technology Professionals

12. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

13. There have been no incidents of NHS Borders staff members or personnel being let go due to issues surrounding cyber security governance.

14. There are no vacancies for cyber security positions within NHS Borders.

15. NHS Borders is in the process of implementing mandatory training in Cyber Security for all staff. Training requirements for staff working in IT/Cyber security roles are assessed as part of yearly appraisal and revised to reflect the evolving nature of the industry.

16. NHS Borders does not have a budget for public relations related to cyber-attacks – therefore, spend is nil.

17. NHS Borders has a Senior Information Risk Officer, which is a Director level appointment that reports to the Board.

18. The board undertakes regular internal and external audits on IT/Cyber Security. The last Network and Information Security Regulations 2018 Audit was undertaken in Aug 2022, these are yearly audits.

19. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

20. Under Section 24 (1) of The Freedom of information (Scotland) Act 2002, NHS Borders considers that disclosure of this information would not be in the interest of the Boards' security. * See note below.

* Disclosing details about Cyber incidents, Operating Systems, Top Cyber Security Risks, Patch Management Cycles, Board Briefings, Staff Training and Cyber Security Vacancies could allow individuals to assess the strength of our defences. The public interest arguments against disclosure under Section 31 (1) (a) are similar. Any attempt to hack into an IT system is a criminal offence. Disclosing this information could aid, and indeed encourage, a criminal who was intent on launching an attack on the organisations ICT systems and could expose the Board to potential threats such as targeted e-crime.

If you are not satisfied with the way your request has been handled or the decision given, you may ask NHS Borders to review its actions and the decision. If you would like to request a review please apply in writing to, Freedom of Information Review, NHS Borders, Room 2EC3, Education Centre, Borders General Hospital, Melrose, TD6 9BS or foi.enquiries@borders.scot.nhs.uk.

The request for a review should include your name and address for correspondence, the request for information to which the request relates and the issue which you wish to be reviewed. Please state the reference number **28-23** on this request. Your request should be made within 40 working days from receipt of this letter.

If following this review, you remain dissatisfied with the outcome, you may appeal to the Scottish Information Commissioner and request an investigation of your complaint. Your request to the Scottish Information Commissioner should be in writing (or other permanent form), stating your name and an address for correspondence. You should provide the details of the request and your reasons for dissatisfaction with both the original response by NHS Borders and your reasons for dissatisfaction with the outcome of the internal review. Your application for an investigation by the Scottish Information Commissioner must be made within six months of your receipt of the response with which you are dissatisfied. The address for the Office of the Scottish Information Commissioner is, Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife.