

Request Reference: 3628

FOI Request dated 07/04/2026 –

Under the Freedom of Information Act, I would like to request the following information for each calendar year from 2020 to 2026 inclusive:

- 1. The number of cyber security breaches that have being identified that were found to be a result of a malicious threat actor (i.e. not accidental data breach)*
- 2. The breakdown in high-level causes of these breaches as identified by cyber security incident response teams (CSIRTs), for example (but not limited to) unpatched software/hardware, lack of multi-factor authentication (MFA), leaked user credentials, lack of in-transit encryption, etc*
- 3. The number of breaches that occurred that were attributed to a previously known vulnerability to the organisations hardware, software, policies, or processes, for example where system was known to be at risk due to being unpatched or out of support, or security controls were recommended but not enforced, and was defined within the resulting incident response report.*
- 4. The estimated combined costs incurred as a result of cyber security breaches defined in request number one in each year.*

Response

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at s1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at s1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of the FOIA requires that we provide the applicant with a notice which: a) states that fact; b) specifies the exemptions in question and c) state (if that would not otherwise be apparent) why the exemption(s) applies.

The University of Hull neither confirms nor denies that it holds information relevant to this request by virtue of the following exemptions; -

- Section 24(2) (National Security)
- Section 31(3) (Law Enforcement) of the Act.

Confirming or denying whether the requested information is held would, in itself, be likely to prejudice national security and law enforcement functions. In particular, it would risk revealing the extent to which the University has been subject to malicious cyber activity, the effectiveness of detection or incident response arrangements, and levels of exposure to criminal or hostile threat actors. Such confirmation could also be combined with other publicly available information, increasing the risk of harm through a “mosaic effect”.

Both exemptions are qualified and the University has therefore considered the public interest. While there is a recognised public interest in transparency and understanding cyber security risks in the public sector, this is outweighed by the strong public interest in safeguarding national security, preventing and detecting crime, and protecting the effectiveness of security and investigative measures. These considerations apply regardless of the historical or high-level nature of the request.

Accordingly, the University maintains a neither confirm nor deny position under sections 24(2) and 31(3) of the Freedom of Information Act 2000.