UK Research and Innovation

[redacted]

5 May 2026

Dear [redacted]

Freedom of Information request: FOI2026/00285

Thank you for your Freedom of Information request received on the 4 April in which you requested the following:

Your request:

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.*

Our response:

I can confirm that UK Research and Innovation (UKRI) does hold some information relevant to your request. Please see the information below.

Please note, UKRI's incident tracker does not contain a field that explicitly marks "malicious threat actor" or "accidental". Where an incident has been classified, this was determined through high-level keywords recorded in the incident tracker and not by a specific flag or field. Data provided for 2026 is correct up to 13 April 2026.

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)*

Year	Number of Breaches
2020	2
2021	0
2022	14
2023	18
2024	26
2025	20
2026	6

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*

Year	Phishing / Social Engineering	Credential compromise / Unauthorised access	DoS / DDoS	Misconfiguration / Exposure	Malware	Third-party / Supply chain
2020	1	1	0	0	0	0
2021	0	0	0	0	0	0
2022	6	3	4	1	0	0
2023	0	0	13	5	0	0
2024	13	7	4	2	0	0
2025	12	4	0	1	1	2
2026	2	2	1	0	0	1
Total	**34**	**17**	**22**	**9**	**1**	**3**

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.*

   We estimate that the cost of complying with this section of your request would exceed the appropriate statutory limit as specified within Section 12 of the FOIA which for UKRI is set at £450. This represents the estimated cost of 18 hours of staff resource on locating, retrieving and extracting the information.

   To gather this information, it would be necessary to review the incident log or final report for each individual incident. Given the length of these documents, the time it would take to locate the relevant parts, interpret and cross-check the information is expected to be 1-2 hours per incident.

   Consequently, UKRI is not obliged under Section 12 of the FOIA to process this section of your request further.

4. *The estimated combined costs incurred as a result of cyber security breaches defined in request number one in each year.*

   This information is not recorded and therefore not held.

Your rights

If you have any queries regarding our response please do let us know. If you are dissatisfied with the handling of your request, you have the right to ask for an internal review, explaining which elements of this decision you disagree with and why. Internal review requests should be submitted within 40 working days of the date of our response and should be addressed to:

Head of Information Governance
Email: foi@ukri.org

Please quote the reference number above in any future communications.

If you are still not content with the outcome of the internal review, you may apply to refer the matter to the Information Commissioner for a decision. Generally, the ICO cannot make a decision unless you have exhausted the review procedure provided by UKRI. The Information Commissioner can be contacted at: www.ico.org.uk.

If you wish to raise a complaint regarding the service you have received or the conduct of any UKRI staff in relation to your request, please see UKRI's complaints procedure[1].

[1] https://www.ukri.org/who-we-are/contact-us/make-a-complaint/#skipnav-target

Yours sincerely,

[redacted]
Information Governance
Information Rights Team
UK Research and Innovation
foi@ukri.org | dataprotection@ukri.org