

Freedom of Information – Response – 27148

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)

During the reporting period, zero cyber security breaches were identified that were the result of a malicious threat actor.

The organisation continues to experience a high volume of attempted malicious activity, all of which is routinely detected and blocked by security controls. Over a typical 30-day period, this includes approximately 4 million emails processed and around 1.26 million attempted attacks blocked. These figures demonstrate the effectiveness of our preventative security measures in stopping threats before they result in a 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

N/A

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.

N/A

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

N/A.

