ICO Disclosure Log – Response IRQ0677245

Information request

I write in response to your email of 13 April 2017 in which you submitted a request for information to the Information Commissioner's Office (ICO). Your request has been dealt with in accordance with the Freedom of Information Act 2000 (FOIA).

Your request

"1. How many reports of cyber-attacks at schools has the ICO received in 2015? 2016? So far in 2017?
2. For each year, can I have details of the results of the attacks did it result in a data breach? Was money lost (and if so how much)?
3. For each year, can I have a breakdown of the motive of the attack i.e. terror? Financial crime? Political cyber crime?"

Our response

I can confirm we hold information that falls in the scope of your request.

Firstly it may be helpful to explain that although casework can be categorised by sector, these are quite broad categories. We do not hold a sector solely for schools, these would be categorised under the 'Education' sector. However, this also includes universities and other educational institutions. For the purposes of your request I have excluded details of incidents relating to any organisations other than schools.

The way we categorise the type of data security incident has also changed in the 2016/17 financial year. Prior to this cyber security incidents would be categorised under the broad heading of 'Insecure webpage (including hacking)'. As of 2016/17 we record a more detailed breakdown of cyber security incidents. These categories now include: 'Cyber incident (exfiltration)', 'Cyber incident (key logging software)', 'Cyber incident (phishing)', 'Cyber incident (other – DDOS etc.)' and 'Cryptographic flaws (e.g. failure to use

HTTPS; weak encryption)'.

In order to locate the information you have requested we have individually examined the self-reported data security incident casework which falls under the above cyber incident category types, in the 'Education' sector, that we have completed in 2015, 2016 and 2017 to date.

I will now address each of your requests in turn.

"1. How many reports of cyber-attacks at schools has the ICO received in 2015? 2016? So far in 2017?"

As explained above we searched for data security incidents in the 'education' sector and which the type was categorised as *'Insecure webpage (including hacking)'* in the 2014/15 and 2015/16 financial years and any of the new cyber incident category types outlined above for 2016/17. We did not consider incidents that related to educational establishments other than schools. Additionally as you specified 'cyber-attacks' we did not include incidents reported where, for instance, students at the school gained access to staff only areas of their network due to incorrect/out of date access permissions being set. We would consider these to be 'access control' issues rather than cyber-attacks. However, we have included instances where, for instance, third parties have 'actively' sought to compromise systems by hacking teacher user accounts etc.

Based on these criteria, the number of cyber-attacks at schools reported to us (by annual year) is as follows:

2015: 4
2016: 8
2017: 2 (+2 open cases)

"2. For each year, can I have details of the results of the attacks did it result in a data breach? Was money lost (and if so how much)?"

Of the above cases, we have closed them with the following case outcomes:

No action for DC: 9
DC action required: 4

One case was closed as a duplicate case as it was referred to our enforcement department. However, this case was later closed as

'No further action'.

Additionally there are two open and ongoing cases.

I have included a link below to a document containing a list and brief description of the case outcomes we use which may be helpful to you.
https://ico.org.uk/media/about-the-ico/documents/1624914/dp-case-outcomes.pdf

In some cases we have not taken further steps to investigate the incidents in question in order to avoid duplication of investigations, as the data controller has referred incidents to the police to investigate under the Computer Misuse Act (which is outside of our remit) and the police would be the primary investigating authority.

In many cases it is difficult to determine whether money was lost, as it is dependent on the level of description of the incident provided by the schools in question. There are only two cases which definitively state that a financial loss was incurred, either by the school itself, or by parties associated with the school (parents, agencies etc).

However, we have withheld the exact loss figure under section 31(1)(g) of the FOIA. This exemption applies when disclosure would or would be likely to prejudice our ability to carry out our regulatory function. This is particularly significant when our investigation has not yet been concluded as is the case with one of the incidents here.

The exemption at section 31(1)(g) of the FOIA refers to circumstances where the disclosure of information "*would, or would be likely to, prejudice – … the exercise by any public authority of its functions for any of the purposes specified in subsection (2).*"

In this case the relevant purposes contained in subsection 31(2) are 31(2)(a) and (c) which state;

"*(a) the purpose of ascertaining whether any person has failed to comply with the law"…* and
"*(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise,*"

Clearly, these purposes apply when the Information Commissioner is considering whether or not a public authority is properly complying with its obligations under the DPA and is determining if

regulatory action is appropriate.

We believe that disclosure of the requested information at this time would be likely to prejudice our ability to effectively carry out our regulatory function.

As you may be aware the exemption at section 31 of the FOIA is not absolute and is subject to the public interest test. I have therefore gone on to consider whether the public interest arguments lie in favour of disclosure or in favour of maintaining the exemption.

Public interest in favour of disclosure

- There is a public interest in the ICO being open and transparent regarding our regulatory activities. Such openness and transparency helps to promote public awareness and understanding of the ICO's regulatory functions.

Public interest in favour of maintaining the exemption

- There is a public interest in the ICO being able to have effective and productive relationships with those that we regulate and that they continue to engage with us in an open, cooperative and collaborative way without fear that information they provide to us will be made public prematurely or, as appropriate, at all.
- There is a further public interest in the ICO providing a cost effective, timely and efficient regulatory function that we feel is best achieved by this informal, open, voluntary and uninhibited exchange of information with those that we regulate. We think that such co-operation may be adversely affected if information of this nature were routinely made public, (particularly in circumstances where a matter is not yet concluded), which would in turn prejudice the ICO's ability to deliver the levels of service required of it.

Having considered the public interest arguments both for and against disclosure we do not think that there is sufficient weight within the arguments to favour disclosure. In light of the above we think that the public interest in maintaining the exemption in section 31(1)(g) outweighs the public interest in disclosure.

"3. For each year, can I have a breakdown of the motive of the attack i.e. terror? Financial crime? Political cyber crime?"

In some cases there is a clear motive, (for instance the use of

'ransomware' and subsequent demands for payment in order to de-encrypt files). However, as above, in many cases it is difficult to determine the motive behind the attack. We are dependent on the level of detail provided by the schools in their reports, and in some cases it is difficult for even the schools to postulate what the motive could have been as there is simply not enough information available, or the attack does not appear to be for a specific purpose. Although in a number of cases, the cyber-attack appears to have been carried out for personal purposes or with the intention to cause 'mischief', there is not enough information to say for certain the motive behind it. These and other incidents where it is difficult to determine the motive I have classified as 'unknown'.

I have provided the figures below:

Financial: 8

Unknown/not enough detail to ascertain: 8

Finally, you may also be interested to note that we do publish some information in relation to the data security incidents we receive and this can be found on our website which includes a csv spreadsheet showing a breakdown of data security incidents by type and sector. This can be found here: https://ico.org.uk/action-weve-taken/data-security-incident-trends/. As mentioned previously, the 'Education' sector will include other educational establishments such as universities in addition to schools.

This concludes our response to your request. I hope the information provided is helpful.