The Directors' Cut

Cyber security
FOI requests

ucisa guidance on FOI requests related to cyber security

September 2019

Context

There has been a recent spate of FOI queries relating to cyber security. The requests have focused on a number of areas:

- How many attacks there have been during a set period?
- What is the impact of such attacks (e.g. how many have caused systems to be infected or services compromised)?
- Where have the attacks have originated from?
- How much is spent on security?
- How much is spent on staff training?

The following provides some brief guidance that may help institutions when considering their responses to such queries (in consultation with their Data Protection Officer). This guidance has been developed using desk research, feedback from ucisa members and discussion with the National Cyber Security Centre.

Freedom of Information Act (FOI)

The various documents and statutory instruments relating to the FOI Act including Scotland specific instruments can be found on the government website.

The Information Commissioner's Office provide guidance on the FOI Act on their website.

According to the ICO guidance the main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to. This is sometimes described as a presumption or assumption in favour of disclosure. The Act is also sometimes described as purpose and applicant blind; however, this poses a challenge when even if the motivation of the requestor is for the benefit of the public interest the information being requested would be of benefit to an individual or organisation in an attack on the institution's data or infrastructure.

Article 17 of the FOI Act describes the circumstances relating to refusal of an FOI request and part II of the act describes the exemptions provided by the Act. Within the context of this guidance articles 2.1.b and 17.3 are relevant and describe that the exemptions in part II of the Act may confer an absolute exemption, or where an exclusion is to be applied, the reason for claiming exclusion outweighs the public interest in disclosing. Article 17.3.a/b states:

> a) *that, in all the circumstances of the case, the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the*

public interest in disclosing whether the authority holds the information, or

b) *that, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.*

Similarly article 16 of the Scotland Act covers refusal of a request and article 18 of the Scotland Act states:

> *Further provision as respects responses to request*
>
> *1) Where, if information existed and was held by a Scottish public authority, the authority could give a refusal notice under section 16(1) on the basis that the information was exempt information by virtue of any of sections 28 to 35 [F638,] 39(1) or 41 but the authority considers that to reveal whether the information exists or is so held would be contrary to the public interest, it may (whether or not the information does exist and is held by it) give the applicant a refusal notice by virtue of this section.*
>
> *(2) Neither paragraph (a) of subsection (1) of section 16 nor subsection (2) of that section applies as respects a refusal notice given by virtue of this section.*

Articles 21 to 44 (25 to 41 Scotland) of Part II of the Act describe the specific Exempt Information Categories. Also note articles 12, Cost of compliance, and 14, Vexatious and repeated request, describes circumstances when a request may also be refused.

Within the context of this guidance article 36 (30 Scotland), Prejudice to effective conduct of public affairs and article 31.1.a (35.1.a Scotland), the prevention or detection of crime, should be considered.

Responding to cyber security related FOI requests

Each institution must judge whether they feel comfortable releasing information relating to cyber security. Careful consideration should be given when the following categories of information are requested:

- makes and models of network equipment and software;
- makes, models and operating software of server and other infrastructure;
- software and tools used in connection with cyber security;
- infrastructure and software used in connection with access and authentication;
- physical security devices and arrangements;
- the detail of successful and unsuccessful cyber security attacks.

It is recommended that colleagues within ICT departments who are asked to provide such information work closely with the Data Protection Officer(s) within the institution to develop good awareness and understanding of the risks associated with disclosing cyber security related information. This will help the

institution's DPO in responding to requests and becoming familiar with the reasoning and justification of applying the relevant exemptions.

The information requested within cyber security related FOI requests will typically fall within two broad categories: information on the detail of attacks and/or security infrastructure, quantitative information relating to numbers and types of attacks.

In the case of requests related to the detail of attacks and/or security infrastructure, each request will need to be assessed. However, institutions may feel that the exemptions within the Act (under articles 36 and 31.1.a) provide justification that the public interest in disclosing the information is outweighed by the disclosure being prejudicial to the effective conduct of the institutions public affairs, and/or the prevention or detection of crime.

Specifically, making public previously successful or unsuccessful attack vectors, or the disclosure of information about the institution's security infrastructure and systems, could provide individuals or groups with information that could aid in an attack on the institution.

There are a number of examples where the Commissioner has ruled in favour of the public body which has withheld information about specific attacks, even where it has been acknowledged that same body concerned has been the subject of cyber attack. It is therefore always worth checking to see whether recent rulings by the Commissioner may support your institution's viewpoint.

For example, in reviewing an appeal by a complainant against the Department for Education, the Commissioner noted that responding to a request for a detailed breakdown of the number of cyber attacks, the nature, and effects of the attacks is likely to be more useful to malicious actors. Further, the Commissioner concluded that:

> **"Confirming or denying whether information is held in relation to this part of the request would reveal something about the way cyber attacks are recorded including whether or not certain details about the nature and effects of attacks are held. A confirmation that information is held for example may give an indication to the success or otherwise of an attack. A denial on the other hand may indicate vulnerabilities in the system or that a particular type of attack was unsuccessful. The Commissioner recognises that terrorists and other malicious actors can be highly motivated and may go to great lengths to gather intelligence. Therefore, although seemingly harmless, confirming or denying whether information such as a monthly breakdown of the number of recorded cyber attacks, the nature, and effects of those attacks is held, may assist malicious actors when pieced together with existing or prospectively available information whether gathered lawfully or not."**

In compiling a response that may rely on exemption 31 (1) (a), institutions could draw on the Commissioner's response above and highlight that:

- **disclosure of details of successful attacks would increase any potential vulnerability to cyber-attack and increase the risk of future successful attacks;**

- **disclosure would provide a malicious third party with information which may assist them in carrying out a criminal act against a public body (including the institution concerned);**
- **hackers or other malicious parties may draw upon information gathered from a wide range of sources to derive information about an organisation's cyber security arrangements;**

Details of successful attacks would provide useful confirmation to malicious third parties about which of their methods of attack have been successful.

Colleagues have reported that many requests received are worded very poorly. In such circumstances, you may choose to respond according to article 1.3.a of the Act and request further information in order to be able to identify and locate the information. For example, in the case of the question of how many attacks in a set period, the definition of attack is ambiguous. The requestor may or may not be interested in attempts by 'bots' to probe the network which are detected and prevented by the Intrusion Detection System/Intrusion Protection System and may run into the hundreds of thousands over a period of time. Similarly phishing emails and other emails containing malware could be considered an attack.

The combination of a poorly worded request and what may be considered as incomplete records may create the temptation to respond that the information is not held; however, consideration should also be given to the potential interpretation of this and the conclusion being drawn that the institution is not operating what may be reasonably considered as good practice. In other words, responding in this way could result in the requester inferring that the institution is not aware of when it is being attacked, is not analysing log files, is not recording known successful attacks and is not learning the lessons of the attacks. It is reasonable to expect that an IDS/IPS system will record the number of events, email filters may report the number of phishing emails and emails containing malware detected. It could also be considered that there will be a number of "attacks" that are not identified and recorded by automated defence tools, so, given the ambiguity of the question, there is likely to be an argument made to state that not all the information is not available, whilst providing what quantitative information is available.

Depending on the wording of the request you may chose to respond with either actual or estimated/extrapolated figures that are available within your IDS/IPS, automated email filters and similar systems. A general statement such as the following could also be considered:
Every internet connected site, including our own, is subject to probes and attacks from a wide range of parties. We take a range of approaches to detect and prevent such activity. It is not our policy to confirm the number of attacks since:

a) ***What is meant by a cyber attack varies;***
b) ***Confirmation the number of detected attacks may indicate the success (or otherwise) of attacks by malicious parties. This information could be useful to such parties in assessing the strengths and weaknesses of our security measures.***

When considering questions such as how much is spent on cyber security and how much is spent on staff training the challenge is to provide accurate figures; spend on some items to maintain security is not always accounted for under a cyber security heading. For example, the regular maintenance of software using patches or configuring a network to optimise security.

The Scottish Government, in responding to a similar request, suggested that it was unable to give an exact figure but highlighted the amount budgeted for cyber security activities.

With regards to staff training spend, cyber security should be the concern and responsibility of the whole institution but delivering an effective security regime will rarely be quantified. A variation on the following responses may be considered appropriate:

> *Securing IT systems is a requirement of most of the service provisions and the proportion of the contract cost relevant to securing the respective systems is not broken down within each contract.*
>
> *The cost of mandatory cyber security awareness training is not available as cyber security training is one of many training packages provided to staff within the staff training programme. The content for the cyber security awareness training has been developed using a training package provided free to the sector as part of the institution's ucisa membership.*

Conclusion

Each individual institution needs to carefully consider how they might respond to cyber security FIO requests, in conjunction with advice from their Data Protection Officer. To aid this process, ucisa will continue to share guidance on this topic, for the benefit of the ucisa membership and the wider sector.

Authors
Peter Tinson, Executive Director, ucisa
Anna Mathews, Head of Policy and Projects, ucisa
Board of Trustees, ucisa

With thanks to: The National Cyber Security Centre and Bruce Roger, Head of Infrastructure Services, University of Strathclyde

Photograph by Jeni Brown, Head of Digital Skills Lab, London School of Economics and Political Science

ucisa
13 Banbury Road
Oxford OX2 6NN

Tel: +44 (0)1865 283425
Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk
www.ucisa.ac.uk

Registered Company No.
09349804