Freedom of information requests concerning it security issues, attacks, ransom and malware and related topics

Introduction

London Borough of Newham (LBN) has a very robust IT security system. We use all the necessary products and tools to keep our systems safe and secure. We update them regularly and we comply with the relevant guidance and codes of practice. We have a duty under the UK GDPR regulation and Data Protection Act 2018 to keep people's personal data safe and secure and we comply with that duty.

Although the council needs to show that it can do this and will comply with its obligations, at the same time we must be careful that too much transparency does not cause damage. Most people are honest, and law abiding and don't intend to misuse information to cause harm. There are criminals who try and exploit system weaknesses to cause damage or make money. Under Freedom of Information, giving information to one honest requester is the same as publishing it to everyone in the world. If we provide information that tells criminals when we last updated our security software for example, they could use that to exploit any known weaknesses and try and hack our systems. The council managed a vast amount of personal data because we carry out so many functions. We have a lot of very sensitive data – for example about care we provide to vulnerable adults, or casework for childcare social workers. The council must take all necessary steps to make sure we keep it this data safe and secure. This means not telling people information that would allow criminals to gain unlawful access to our systems that may allow them access to the data we hold.

Freedom of Information Act requests

1. IT security Issues. We are frequently asked for information about IT security issues in LBN. We are often asked about what IT security systems we have in place, the suppliers and versions of our IT security, how often we update and amend our security, whether we have identified issues or vulnerabilities and what we have done to strengthen those. The council has considered these issues carefully and we have decided that we do not release this information. This is because we consider it is exempt under section 31 of the Freedom of Information Act 2000. We have explained why below. **Refusal Notice Section 31(1)(a) – Law Enforcement**

Section 31(1)(a) says that we do not need to provide information that would be likely to prejudice the functions of law enforcement - the prevention and detection of crime. LBN believes that releasing this information would increase the likelihood of...

- criminals using the information to target attacks against council systems. For example, knowing when we last updated a security system would allow criminals to know what vulnerabilities existed at that time and target attacks on those. It is important LBN does not do anything that would allow personal data it holds to be accessed illegally.
- knowing if LBN's systems do not have vulnerabilities will increase the chances of other more vulnerable organisations being targeted by criminals

Public Interest Test:

As Section 31 is a qualified exemption we need to consider the public interest test.

Factors in favour of disclosure

- It would help transparency and accountability of the council
- It would reassure people about whether our systems are vulnerable or not
- It would provide information about how effective our security systems are

Factors in favour of withholding

- There is an inherent public interest in crime prevention
- There is public interest in avoiding the costs (financial, distress, inconvenience, publicity, regulatory) associated with any attacks
- There are public interests in preventing any threat to the integrity of council data
- There is public interest in ensuring the council can comply with its duties to take all necessary steps to safeguard data

We believe that the balance of public interest lies in upholding the exemption and not releasing the information.

2. Malware, ransom attacks etc.

We are also often asked questions about malware, ransom ware, attacks and the like. We are asked if we have had any cyber-attacks, and how many, if they have succeeded and what actions we have taken. We can be asked if we have been the victim of ransomware, whether attacks were successful, if we paid ransoms, how often, when, to whom and for how much. We have decided that we do not tell requesters if we hold this information or not. Under Freedom Information Act this is called a 'neither confirm nor deny' response. We can do this under section 31 of the Act. We have explained why below.

Refusal Notice Section 31(3) – Law Enforcement

The council believes that telling requesters if we hold information about cyber-attacks, ransom ware etc will cause damage. This is because saying if we do or do not hold information would give cyber criminals insight into vulnerabilities which may,

or may not, exist. This would we likely to damage our cyber security systems and plans. Therefore, we use the exemption in section 31(3). This allows us to refuse to confirm or deny if the information is held. The council is allowed to refuse to say if it holds information about this or not. When we use a neither confirm or deny response you should not assume that we do, or do not, hold any information.

Section 31(3) is a qualified exemption which means we must do a public interest test where we compare the public interest for and against disclosing. The public interest test is not about whether we should disclose any information that we might hold. It is a test of whether we should say if we hold the information or not.

Factors in favour of confirming or denying if we hold relevant information.

- It would help transparency and accountability of the council
- It would reassure people about whether our systems are vulnerable or not
- It would provide information about how effective our security systems are

Factors against confirming or denying if we hold relevant information.

- Saying if we hold information would provide information about how effective our security systems are. This would be likely to give cyber criminals insights into the strengths of the council's cyber security and any potential weaknesses that may exist. This would increase the chances of cyberattacks. One of the reasons that cyber security measures are in place is to protect the integrity of personal and sensitive personal information so increasing the chances of an attack would have potentially serious repercussions.
- If the council confirms that it holds a lot of information then this could show criminals its systems are particularly vulnerable, encouraging attacks
- If the council confirms that it holds little information this could either show it has poor reporting and recording procedures which will encourage an attack, or it could show it has robust procedures which could encourage an attack to try out criminals' new techniques or could encourage criminals to target other councils' systems which would increase crime elsewhere
- There is public interest in complying with our legal obligations to keep personal data secure and to take appropriate measures which includes keeping areas confidential where necessary

We believe that the balance of public interest lies in upholding the exemption and not confirming or denying if we hold this information.

Your Rights

If you have made a FOI request and you are not happy with how your request was handled, you can request an Internal Review within 2 months of being directed to this page - email to informationrightsteam@newham.gov.uk. Please quote your case reference number.

If you are not satisfied with the Internal Review outcome you have the right to contact the Information Commissioner's Office at casework@ico.org.uk, telephone 0303 123 1113, or post to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. The ICO website www.ico.org.uk may be useful Information Commissioner's Office (ICO) .