Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 6405

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

17 November 2020

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to cyber-attacks.

You asked:
A list of all cyber-attacks (both failed and successful) on NHS hospitals falling under your remit, in each year since 2015 (including broader cyber-attacks which include these hospitals). Where possible, please could you split the data as follows:

- *Ideally, I am requesting **only** those cyber-attacks identified as or suspected of a) coming from a source within Russia or China; or b) emanating from any individual(s) or group(s) known to have, or suspected of having, links to the Russian or Chinese state. In each instance, please could you make clear which country the attack relates to.*
- *If this is not possible, please could you make clear whether an attack is thought to have come from inside/outside the UK.*

In each instance, I am also requesting the following information:

- ***The severity** of the attack, where it has been noted (e.g. low, medium, high).*
- ***The outcome** of successful attacks. For example: were documents stolen (and how many)? Was confidential data stolen (and how much)? Were any operations or other NHS processes cancelled or delayed as a result (and how many)?*
- ***The cost** to the NHS, where that cost is easily deductible/accessible. This could include but is not limited to a) delayed or cancelled operations, lost data, etc.; b) the security/staffing cost of defending against an attack; c) any consequent legal costs e.g. lawsuits filed successfully against the NHS as a result of personal data theft. If this part of the request is unduly onerous, please disregard.*

Trust response:
The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to this question as providing this could compromise the security of the Trust's network / data and might materially cover activity which forms part of ongoing criminal investigations
The information which has been withheld is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act. The relevant parts of the ICO guidance on the subject (https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf) run as follows:
31.—(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures. It is the view of this trust's Information security function that disclosure of the information above would prejudice our ability to resist cyber-attacks, etc. on our systems.