Freedom of Information Request: Our Reference CTHB_358_16

You asked:

1. Has your organisation been a victim of a cyber attack in the last two years? If yes, how many times?
2. Has your organisation been a victim of a ransomware attack in the last two years? If yes, how many times? In each case, was a ransom paid and if so how much was paid?
3. For each of the cyber and ransomware attacks, please provide a summary of the incident. This should including details of who was targeted, how they were targeted, what the immediate impact was, for instance was patient or staff data targeted, and if so in what way and how many people's data was affected? For each of the attacks, please also detail whether the police became involved, and whether the perpetrator or perpetrators were caught?

Our response:

Cwm Taf University Health Board neither confirms nor denies that it holds information falling within the refines of your request. The duty in s.1(1)(a) of the Freedom of Information Act 2000 does not apply, by virtue of s.31(1)(a), and s.38(1)(a)&(b) of the Freedom of Information Act 2000. These sections exempt us from our duty to say whether or not we hold the information you asked for. This should not be taken as an indication that the information you requested is or is not held by the organisation.

Cwm Taf University Health Board recognises its duty to protect the public and individuals, and we will not jeopardise this duty by confirming or denying if we hold information as, in our opinion, this would weaken our ability to protect our patients, staff and other service users.

Confirming or denying whether any information is held would reveal details about our security measures into the public domain and could make this information accessible to criminals and cyber terrorists and subsequently compromise public and individual safety. The Health Boards protective security measures that exist are there to protect our systems which are used to directly assist with the provision of patient care. It has been established that anyone who may be planning cyber-attacks are known to conduct extensive research into the opposition they might face, and confirming or denying whether any information is held about the security of our systems, no matter how innocent such requests may appear, may enhance the capability of cyber terrorists and hackers to carry out such attacks.

Confirming or denying whether any information is held could enable hackers and cyber criminals to gain knowledge about the Health Boards capabilities and IT security measures, and this could enable them to plan attacks where they perceive a lower level of security resource exists. This exposes our IT systems to greater risk and therefore, constitutes a risk to both public and staff, as our systems are used to provide patient care.

However, by neither confirming nor denying that any information is held, those with the inclination to commit cybercrime will not have access to knowledge about any increase of threat to specific areas or individuals, and they will be prevented from exploiting such information in order to target those areas or individuals.

Section 31 – Law Enforcement of the Act states that:
31(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime

Section 38(2) – Health and Safety of the Act – states that:
38(1) Information is exempt information if its disclosure under this Act would, or would be likely to –
(a) endanger the physical or mental health of any individual, or
(b) endanger the safety of any individual.
(2) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, have either of the effects mentioned in subsection (1).
The UHB therefore believes that the greater public interest in neither confirming or denying outweighs any arguments for disclosure.