Freedom of Information Request: Our Reference CTMUHB_367_21

You asked:

1. **In the past three years has your organisation:**
   a. **Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)**
      i. **If yes, how many?**
   b. **Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)**
   c. **Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)**
   d. **Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?**
      i. **If yes was the decryption successful, with all files recovered?**
   e. **Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?**
      i. **If yes was the decryption successful, with all files recovered?**
   f. **Had a formal policy on ransomware payment?**
      i. **If yes please provide, or link, to all versions relevant to the 3 year period.**
   g. **Held meetings where policy on paying ransomware was discussed?**
   h. **Paid consultancy fees for malware, ransomware, or system intrusion investigation**
      i. **If yes at what cost in each year?**
   i. **Used existing support contracts for malware, ransomware, or system intrusion investigation?**
   j. **Requested central government support for malware, ransomware, or system intrusion investigation?**
   k. **Paid for data recovery services?**
      i. **If yes at what cost in each year?**
   l. **Used existing contracts for data recovery services?**
   m. **Replaced IT infrastructure such as servers that have been compromised by malware?**
      i. **If yes at what cost in each year?**
   n. **Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?**
      i. **If yes at what cost in each year?**
   o. **Lost data due to portable electronic devices being mislaid, lost or destroyed?**
      i. **If yes how many incidents in each year?**

Cwm Taf Morgannwg 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 Morgannwg 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.

2. **Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?**

   Yes.

   a. **If yes is this system's data independently backed up, separately from that platform's own tools?**

      Cwm Taf University Health Board has deemed that the information requested is exempt from disclosure under Section 31(1)(a) and Section 38(1)(a)&(b) of the Freedom of Information Act 2000 (the Act).

      The UHB recognises its duty to protect the public and individuals, and we will not jeopardise this duty by providing this information, in our opinion, this would weaken our ability to protect our patients, staff and other service users. We have also considered the harm which will or will be likely to arise from the release of this information along with information already in the public domain.

      Section 31(1)(a) of the Act provides that information which is not exempt by virtue of Section 30 (criminal investigations and proceedings) is exempt if its disclosure would, or would be likely to, prejudice the prevention or detection of crime. In guidance, the Information Commissioner's Office has advised that Section 31 amongst other things, prevents information being disclosed that would increase the risk of the law being broken. In addition, it can be claimed by any public authority. The UHB is relying upon this exemption as it considers that releasing this information about our IT systems, would in the present climate, make it more vulnerable to crime.

      Therefore the UHB considers that the public interest in withholding the information outweighs any arguments for disclosure, therefore protecting the UHB from potential criminal activity.

3. **Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.) –**
   a. **Mobile devices such as phones and tablet computers**
   b. **Desktop and laptop computers**
   c. **Virtual desktops**
   d. **Servers on premise**
   e. **Co-located or hosted servers**
   f. **Cloud hosted servers**
   g. **Virtual machines**
   h. **Data in SaaS applications**
   i. **ERP / finance system**
   j. **We do not use any offsite back-up systems**

   The Health Board has a backup policy in place that backs up both locally and offsite.

4. **Are the services in question 3 backed up by a single system or are multiple systems used?**

   Please see response to question 3a.

5. **Do you have a cloud migration strategy? If so is there specific budget allocated to this?**

   This is nationally driven by Digital Health and Care Wales (DHCW). For further information, you may wish to redirect this element of your request to DHCW directly via the following link Freedom of information - Digital Health and Care Wales (nhs.wales).

6. **How many Software as a Services (SaaS) applications are in place within your organisation?**
   a. **How many have been adopted since January 2020?**

   Please see response to question 5.