**In no more than 500 words**, address the following TWO questions and their parts

1. *What is a data breach?* Undertake some online research to identify a recent example (***from the last 6 months***) of a data breach
   1. Describe the characteristics of your example of a data breach (How did it occur and what was most significant about it? **(2.5 marks)**
   2. Explore your case in relation to the definitions used in week 1 and week 2 of INF30020 and synthesise common features to present what you consider to be the most significant aspects of a good definition of data breach. **(2.5 marks)**
2. *Bunnings data breach Wk11 & Wk2.* Undertake some additional reading
   1. With consideration for the Mike Van Stone paper – [Mistakes Happen -](https://swinburne.instructure.com/courses/44640/pages/m001-readings-and-resources) clarify how unintentional data loss fits your understanding of data breach with reference to the our first Bunnings case: Bunnings 2019  **(2.5 marks) ~~(similar to Shadow IT ig as he took the data home with him to make database for his review..link both to the paper and also to the bunning employee’s words. Then end it by saying that data (sensitive) has still been used in an unauthorized manner where he did… which is why it is still considered as a data breach)~~**
   2. Why do you think it is that public disclosure and the notification of data breaches is now seen as an important part of the information security environment? Discuss with reference to John Pironti’s paper, [Five Key Lessons Learnt](https://swinburne.instructure.com/courses/44640/pages/m001-readings-and-resources) and Bunnings 2022 data breach **(2.5 marks) (hold them accountable to standards and policies, ensuring orgs use proper standard and policies to protect against data breaches so as not to damage their reputation ---like ensuring the bunning employee knew what he could and could not do; ensuring orgs know what assests to protect and how to do so ---like knowing certain data being copied/ accessed by unauthosired employee on bunning and checking shodan properly like …. To tack and see whether their info is there or not by notification system or smth, to ensure no stone leaves unturned and they don’t miss anything…; realize that most attacks are actually known and understood vulnerabilities and threats and thus focus on ensuring known remedies are already being used---like maybe user acls or other security features to prevent the employee from accessing the data; they can be attacked by an employee from their vendor company and thus should trust but still verify information being accessed by their vendors---like bunnings could be vendor of any company and thus the leaked information could be used to scam that company by pretending to be from bunnings; customer’s expectionationa are rising and tech is being simpler to implement and thus all of these allows companies to easily keep upto date with their security and also assure their customers)**

**(flexbooker was like vendor type as bunnings relied on it for its service)**

Make sure to reference your sources correctly (both the in-text references and the details in the reference list). References are not included in the word count/page limit. Please use [Swinburne Harvard Referencing Style (Links to an external site.)](https://www.swinburne.edu.au/library/search/referencing-guides/harvard-style-guide/) (check out the [Swinburne Online Library. (Links to an external site.)](https://www.swinburne.edu.au/library/search/referencing-guides/harvard-style-guide/) if you are unsure).

1. In simplest terms, data breaches are security violations where the confidentiality of information assets (like database files, business procedures, policies, back up plans, etc. (reference: <https://www.staffnet.manchester.ac.uk/igo/records-information-management/information-asset-register/> )) of an organization has been lost by enabling an unauthorized person to view, access, copy, transmit or even steal the data.
   * 1. One such example of this has been the data security incident that occurred in Shields Health Care Group, Inc. There, an unauthorized individual had gained access to their system between 7th to 21st March of this year and obtained information asset, which had been the approximately 2 million (https://www.bleepingcomputer.com/news/security/shields-health-care-group-data-breach-affects-2-million-patients/) patients’ “full name, Social Security numbers, Date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information” (https://shields.com/notice-of-data-security-incident/).All of these could be used to commit Identity thefts, phishing, scamming and social engineering attacks on these patients who are not only under Shield’s care, but also under the care of its partnered hospitals and medical centers.
     2. Comparing the Shield’s breach to definitions of data breaches, I believe that the most significant aspects of a good definition can be said as follows: loss of confidentiality of sensitive, personal, or private information asset of an organization due to any form of intentional or unintentional unauthorized access, including view, modification, copy, transmission, deletion, etc. of the said information. But it should not be linked to the level of harm the action would cause to the organization (as said in the definition given in week 2 class activity slide) as no matter how small or large the impact, it would still be considered as data breach.
2. A) In the Bunnings 2019 case, the data breach had been caused by the employee setting up the database, which had contained information about both staff and customers, on his home computer and exposed it online. This is similar to the “Shadow IT” point mentioned on Mike’ paper on “Mistakes happen” where a physician ended up exposing patient details while trying to disconnect his personal server from hospital’s network. Even though the motive behind both of the actions had been non-malicious, they still caused an outcome where confidentiality of sensitive information had been lost as their actions had ended up allowing unauthorized users to view, copy, transmit the said information (the staff and customer information for Bunnings’ employee’s case and patient data for the physician’s case), etc. Thus, following the definition of data breach I had mentioned before, they have still committed data breach.

B) Considering John’s paper on 5 key lessons learnt and the Bunnings 2022 Data Breach, we can find the following points:

I) it holds the companies accountable, ensuring that they use proper standard and policies to protect against data breaches so as not to damage their reputation;

II) it helps companies find out all the assets that they need to protect and thus find the best way to protect them without missing anything;

III) realize that most attacks are actually common, known, well –understood threats and have readily available solutions;

IV) help them realize that they still need to verify the information moving between them and their vendors or partnered companies and ensure that they are following proper information security standards and policies

v)it allows them to keep upto date with the security features and also maintain customer’s trust by knowing what to do to not only prevent data breach but also what steps to take in case a breach occurs (as seen in Bunnings 2022 Data Breach case)

1. (Need to write part 2 a b properly and also fix the reference fro part 1)

Reference:

<https://www.staffnet.manchester.ac.uk/igo/records-information-management/information-asset-register/>

<https://shields.com/notice-of-data-security-incident/>

https://www.bleepingcomputer.com/news/security/shields-health-care-group-data-breach-affects-2-million-patients/)