1) In simplest terms, data breaches are security violations where the confidentiality of information assets (like database files, policies, backup plans, etc. ***(IGO,2018)***) of an organization has been lost by enabling an unauthorized person to view, access, copy, transmit or even steal the data.

   A. 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 ***(Toulas, 2022)*** 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" ***(Shields Health Care Group, 2022).*** All of these could be used to commit Identity thefts, phishing, social engineering attacks, etc. on these patients under Shield and their partnered hospitals' care.

   B. Comparing the Shield's breach and the definition, 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 unauthorized access, including view, modification, copy, transmission, deletion, etc. of the said information.
   But it shouldn't 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 case, the data breach had been caused by the employee setting up the database, containing 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 where a physician exposed patient details while trying to disconnect his personal server from the hospital's network. Although both actions had non-malicious intention, they still caused confidentiality of sensitive information to be lost, allowing unauthorized users to view, copy, and even transmit the said information. Thus, following the definition of data breach I had mentioned before, they have still committed data breach.

   B) As seen in John's paper, public disclosure and notifications of data breaches are extremely important for several reasons. For instance, they hold companies accountable for data breaches, ensuring that they use proper, up to date standards and policies (so as not to damage to their reputation and also keep customer's trust). Furthermore, it also helps companies find out about all the assets that they need to protect and realize that most attacks are from well-known threats whose solutions the organization already has. Last but not the least, it helps them realize that their vendor or partner companies can also be a source of the attack (as seen in Bunnings case as well where FlexBooker's security breach caused a data breach in their organization too) and thus ensure that proper steps are taken to prevent them.

Reference:

IGO, 2018, *What is an information asset register*, IGO, viewed 10th Aug 2022, <https://www.staffnet.manchester.ac.uk/igo/records-information-management/information-asset-register/>.

Toulas, B, 2022, Shields Health Care Group data breach affects 2 million patients, BleepingComputer, viewed 10th Aug 2022, < https://www.bleepingcomputer.com/news/security/shields-health-care-group-data-breach-affects-2-million-patients/>.

Shields Health Care Group, 2022, Notice of Data Security Incident, Shields Health Care Group, viewed 10th Aug 2022, <https://shields.com/notice-of-data-security-incident/>.