Task 10.1P Ethical Scenario Analysis - Cloud Group 5

1. **What are the possible ethical scenarios/dilemmas that might exist with the usage of your product?**
    - Breach of the database, exposing personally identifiable information (PII)
    - Users' passwords are not stored securely
    - Using user data for unauthorised purposes (purposes other than stated to the user)
    - Limited website accessibility (exclusion of some users)
    - Incorrect information/maintaining correct information on recalled products

2. **For the ethical scenario/dilemma you have chosen:**
    a. Who are the stakeholders in the scenario?
        - The website owner/parent company.
        - The employees of the website.
        - Users who sign up to the website.

    b. What are the facts?
        - Information Technology (IT) manager finds through server maintenance that a Man-in-the-Middle attack has occurred.
        - An anonymous user has been intercepting users commands through the website.
        - The IT Manager has stopped the attack.
        - The IT Manager believes the attack has lasted several weeks.
        - Database manager reveals, from the past four weeks 70% of users requesting local data were existing users and 30% new users.
        - It is estimated that over five hundred user passwords and PII were obtained.

    c. Which facts raise ethical concerns? Why?
        - Users are unaware of their data being taken without consent, meaning if users have used previous information on other websites/apps/devices there is a higher probability of private information continuing to be obtained illegally.
        - All users are unaware of the security of the website, meaning that there could be a preconceived idea of users believing the website is impervious or is rigours in maintaining higher security detection. Users are still under presumed assumption and therefore cannot make an accurate choice in choosing to share private information.
        - IT security only detected the threat through maintenance of the server, not proactively preventing a possible threat. This shows a lack in foresight in how a correlation of more personal data collected creates a higher target from hackers.

    d. What are the rights and duties of each of the stakeholders?
        - The rights and duties of clients include:
            1. Being made aware of the website being hacked.
            2. How long the website was vulnerable to the attack.
            3. Which clients were attacked if not how many presumed to be attacked.
            4. What details were exposed.

5. What can happen with the presumed data breach from the attacker.
6. What actions they should take for other platforms they interact with (change passwords, enable two-factor authentication).
7. What the website's security plan is going forward.

- The rights and duties of the company would be:
    1. To find out who initiated the attack.
    2. To declare that the attack occurred within a public area that is likely to reach most of the users affected (through email accounts, on the website).
    3. How the company would resolve the attack within their community (e.g. through pursued legal action).
    4. An increase in security.

- The employees of the company duties include:
    1. To adjust their overall security operations.
    2. Upgrade or increase their awareness of a known security risk.

e. Does the ACS Code of Ethics and Professional Practice provide any advice on these issues? If so what?
    - The ACS Code of Ethics and Professional Practice provides advice on both the conduct of the business internally and externally:
        1. Honesty: Breaking or misleading public trust within IT is against ACS code, the company must not mislead clients or potential clients willingly. This would be a guideline of how the company should operate if it knowling allows a flaw to be exploited to the detriment of clients.
        2. Competence: ACS code reflects the need to respect and protect stakeholders' proprietary interests within the website, not to misrepresent the company's skills or knowledge and accept responsibility for their work. The competency profile for the company would need to be addressed internally whether they were competent in the security of client's private data and if they have accepted partial responsibility for the failure of security.

f. How would you resolve the dilemma identified in point (c) above? Justify your decision.
    - The company should increase overall security by introducing a dedicated security department or increase the productivity of the department by scaling with the increase of users. Routine security checks across all points of security (firewall, social manipulation) for the company. This would ensue regular checks and a larger understanding of how threats can be expected and thwarted.
    - The company publicly announces on their website and through emailing all users that a cyber attack has occured and potentially all PII has been illegally obtained.
    - The company reveals new security additions to the public and reveals to users that stronger password protection across all media platforms are needed if user passwords were repeated.

- Two-factor authentication is always enabled and not one to be selected by the user of the website. This would ensure the added protection of users personal information is more secure on the front end of the website.

g. How are each of the stakeholders listed in point (a) affected by your decision?
   - The website owner/parent company:
     1. A larger monetary investment would be required for the increase in staff and working hours.
     2. The website would by publicly announcing the attack create a dilemma in how the website/company is perceived with security. This would likely reduce both current and future users on the main website and possibly a reduced interest in any future company products.

   - The employees of the website:
     1. Possibly reduced workers if the sights popularity is affected negatively.
     2. Employees would be required to make additional changes to the website, restructuring how the site is operated and maintained.

   - Users who sign up to the website:
     1. Users would have to come to terms with how they might be affected by the data breach.
     2. They would need to make a decision on passwords security for other platforms and whether to continue using the breached website.

h. What should you do to avoid the dilemma in the first place?
   - The company should invest in a larger department or a dedicated team that maintains security of the business from cyber threats. Illegal activity from hacking should be routinely scanned and stricter pre-emptive measures should be in place. Both the daily security standards and IT security teams should be routinely checking and foreseeing potential attacks while also having a large enough department to make the checks a reality.

i. What federal and/or state legislation currently exists in Australia that could apply in this or other similar situations? Consider any contractual obligations that may be relevant.
   - Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018
   - Cybercrime Act 2001
     - ❖ 477.1 Unauthorised access, modification or impairment with intent to commit a serious offence
     - ❖ 477.2 Unauthorised modification of data to cause impairment
       - ➔ Modification of customer's detail and information requires consent from the customer.
     - ❖ 478.1 Unauthorised access to, or modification of, restricted data

- ❖ 478.2 Unauthorised impairment of data held on a computer disk etc
  - ➔ Modification of customer's detail and information requires consent from the customer.
- ❖ 478.3 Possession or control of data with intent to commit a computer offence

j. What policies and procedures, if any, should be in place at the organisational level, or embedded in your design for the project to address this and other similar issues?

- Our values:
  - ❖ Transparency: helps us build trust with each other and with society by being honest and open about how and what we do.
  - ❖ Integrity: we expect the highest ethical behaviours of ourselves.
- Managing records properly
  - ❖ Personal Information Security: We have a duty to protect the personal information that we collect and retain about people to ensure it is not misused. All employees who have access to or work with personal information must complete relevant training.
  - ❖ Relevant and keep information on track: Keep recording up-to-date will help protect information.
  - ❖ Data integrity: Make sure information is accurate and stored correctly.
- Preventing fraud, bribery and all forms of corruption
  - ❖ It is illegal to bribe. Speak up and report any suspected corruption about fraud, bribery or corruption.
- Keeping safe at work
  - ❖ Safety is always the priority. We should all feel safe to work for company
  - ❖ Treating people equally and Trusting each other