Question 1-A

Affected groups by the Optus data breach

Data breaches are becoming more common, compromising the personal data of millions of people worldwide (Khan, 2019). Striking examples include the Equifax breach, which affected 147 million people, and the Facebook leak, which affected more than 500 million users. Data breaches have negative externalities for consumers, companies, and society as a whole. Impacts include identity theft, reputational damage, declining shareholder value, and erosion of institutional trust (Goode et al., 2017; Hinz et al., 2015). Data breaches also impose regulatory pressure and oversight costs on governments (Romanosky et al., 2011). These events have had a serious impact on multiple stakeholders. Among affected groups, this report identifies customers, shareholders, and government as three of the most impacted stakeholders in the Optus breach case.

Customers

Optus customers whose personal data was compromised are profoundly affected:

- Invasion of privacy and exposure of their sensitive personal information
- If data is misused, the risk of identity theft and account theft is high
- Disrupt daily life and activities, take precautions such as card replacement

Shareholders

Optus shareholders face financial and reputational impacts:

- Investors reacted negatively, with stock prices and market valuations falling
- Reduced dividend payments due to default costs and lost revenue
- Uncertainty about future full financial impact

Government

The government must take urgent response actions:

- Divert significant resources to non-compliance handling and aftercare
- If the reaction is deemed not strong enough, there is a risk of reputational damage
- Address the decline in public trust in the ability to implement data protection

Question 1-B

Carroll's pyramid of CSR

According to Carroll's pyramid model(Carroll, 1991), corporate social responsibility includes four layers of responsibility – economic, legal, ethical, and philanthropic. Economic responsibility refers to profit and financial responsibility. Legal liability involves compliance with laws and regulations. Moral responsibility means doing what is morally right and just. Charitable responsibility includes being a good corporate citizen through voluntary contributions to society.

Economic Responsibilities:

- To customers: Provide affordable and high-quality telecommunications services
- To shareholders: Maintain financial position and deliver satisfactory returns
- To government: Legal and compliant tax payment

Legal Responsibilities:

- To customers: Protect data privacy and security in accordance with regulations
- To shareholders: Regularly disclose the company's operations

- To government: Comply with applicable laws and regulations

Ethical Responsibilities:

- To customers: Business transparency and do not exaggerate business
- To shareholders: Be transparent about the impact of violations and responses
- To government: Open communication and do not hide problems

Philanthropic Responsibilities:

- To customers: Help for families in need
- To shareholders: Compensate some shareholders for losses
- To government: Support stronger industry-wide safety programs

Question 2

How to choose Optimal level of data security

This report mainly uses the cost-benefit principle and the interdependence principle to analyze the optimal data security level.

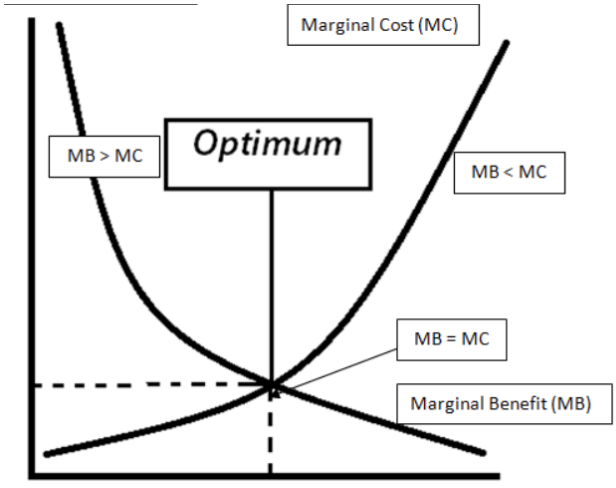
Cost-benefit principle

The cost-benefit analysis involves comparing the additional costs of a higher level of data security with the expected benefits.

For Optus, a higher investment in data security means:

- Marginal cost: system upgrades, staff training, firewall upgrades.
- Marginal benefits: avoidance of potential risks, attracting new customers, stock market gains.

The optimal level is that the marginal cost of the final higher data security investment is exactly equal to the marginal benefit it is likely to receive.



Interdependence principle

The principle of interdependence recognizes the interconnectedness between a business and its stakeholders, and the actions of a company that create positive or negative externalities to others.

Optus should account for how its security produces externalities on interconnected entities like:

- Customers - Identity theft, emotional distress
- shareholders - Falling share price, reputation damage
- government - Investigating incident, regulatory changes

In summary, considering the cost benefits and impact on stakeholders, Optus should rethink the new level of data security to better protect the interests of customers, shareholders and government.

Question 3

Possible legal issues

Data breaches occur frequently, exposing organizations to significant legal risks. Studies have shown that data breaches can lead to issues such as breach of contract, violation of privacy laws, and corporate consumer litigation (Romanosky et al., 2011; Stevens, 2012). The data controller is obliged to protect personal information legally and bear the consequences of its disclosure.

This report will use relevant legislation and precedent to examine the potential legal issues Optus faces under contract law and Australian Consumer Law following a data breach.

Contract Law

Optus previously entered into contractual terms with customers, which included safeguarding the security of their data. This data breach violates contractual obligations to protect customer information.

Relevant legislation:

The Privacy Act 1988 is Australia's primary legislation governing the protection of personal information. The Act sets out a framework for public and private sector organizations to handle personal information responsibly. At the heart of the Privacy Act is the Australian Privacy Principles (APP), which outline standards, rights and obligations relating to the processing, holding, access, correction and use of personal information. Some key principles include:

- Notice of Collection of Personal Information - Organizations must notify individuals at the time personal information is collected.
- Personal Information Security - Organizations must take reasonable steps to protect personal information from misuse, interference, loss, unauthorized access, modification, or disclosure.
- Correction of Personal Information - Organizations must take reasonable steps to ensure that the personal information they hold is accurate, current, and complete, and must correct any information found to be inaccurate.

Relevant case:

Between 23 June 2012 and 15 May 2013, Telstra's electronic form file with customer names, addresses and phone numbers was visible through the Google search engine. Telstra breached privacy laws and industry guidelines by accidentally leaking the information of nearly 1.6 customers and fining A$10,200.

Australian Consumer Law

The data breach violates the ACL's unfair contractual terms. The safeguards advertised by Optus proved to be flawed, and Optus' limitation of liability for security breaches may be legally challenged.

Relevant legislation:

The ACL contains a number of laws on unfair treatment. The most important of these is the provision of unfair contract terms. Under Articles 23 and 24 of the ACL, a contractual clause may be considered unfair if it:

- The company has had a material adverse effect on consumers;
- The company has not protected the legitimate interests of the other party;
- The conduct of the company has led to a significant imbalance in the rights and obligations of the parties to the contract.

Relevant case:

In 2011, Sony's PlayStation Network suffered a severe data breach that affected the personal and credit card information of about 77 million users. Subsequently, the affected users filed a class-action lawsuit accusing Sony of violating the contract with the user and demanding damages. Sony eventually agreed to pay a $15 million settlement to settle the case.

Reference

Carroll, A.B., 1991. The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. Business horizons, 34(4), pp.39-48.

Goode, S., Hoehle, H., Venkatesh, V. and Brown, S.A., 2017. User compensation as a data breach recovery action. *MIS Quarterly*, *41*(3), pp.703-A16.

Hinz, O., Nofer, M., Schiereck, D. and Trillig, J., 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), pp.337-347.

Khan, F.S., Kim, J.H., Moore, R.L. and Mathiassen, L., 2019. Data breach risks and resolutions: A literature synthesis.

Romanosky, S., Telang, R. and Acquisti, A., 2011. Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, *30*(2), pp.256-286.

Stevens, G.M., 2012. Data security breach notification laws.