CSC8101 Penetration Testing

Assignment 1

Created by: Deep shah

Student ID: U1137064

Date: 26 March 2022

Question 1: Part A- Legal Issues

1. You have been retained by a company test the security of their employee database. You successfully enter it and access employees' passport numbers and financial account numbers. An employee discovers your actions, presses charges and you are committed to 5 years imprisonment.

Answer 1: the first statement is true.

The charges that are press are correct according to the **section 408D**. obtaining or dealing with identification information has the maximin penalty of 5 years imprisonment. In above case a person is hired to check the security of the database that person is allowed to penetrate the database but not allowed to view the personal data files of the employees such as passport numbers and bank credentials.

2. You are at the office late one night following an argument with your manager and notice their computer is still on. You guess their password which grants you access to your system. You realize it's not worth doing anything with it, log out and go home. You have not committed an offence.

Answer 2: this statement is not true.

Unauthorized data access carries a maximum penalty of two years under **section 478.1.** Even if we recognize it is not worthwhile to do anything with it, guessing the password and gaining access to the system is a crime.

3. You are performing a security test for a company but go outside the scope of the agreed contract. You find an issue and do what you think is best to fix it, however this fix has affected the reliability and security of the data. You are convicted and receive 2 years imprisonment.

Answer 3: this statement is true.

Going outside the scope of a contract is the same as hacking a system without the consent of the firm, often known as black hat hacking. The maximum penalty for computer hacking and misuse under **Section 408E** is two to ten years in prison. As a result, the above sentence is correct.

4. Bored one evening, you decide to test the security of your favourite website. Within an hour you have gained access to a range of personal data. You are a bit short on cash this week, so figure you could sell those details online. You find a buyer, but you don't end up completing the transaction. You have not committed an offence.

Answer 4: this statement is false.

Penetrating or gaining access to a website without a valid contract or at the very least without informing the website's owner is the same as hacking the site, regardless of whether you want to disrupt the system or only conduct a security check. This action is a criminal offence under **Section 408E**. As a result, the above assertion is false.

5. You are working for a large, multinational company that turns over $20m per year. In your role you inadvertently expose a flaw in the system that exposes your customers health records. You only realise this 1 week after the event, but immediately notify your manager. Your manager does not report it to the OAIC under the notifiable data breach scheme. Your company carries on with its work and does not notify their customers that this occurred.

Answer 5: the above statement is false.

Organizations with a turnover of more than $3 million must be transparent about personal information and management under the **Privacy Act 1988(cth)** and **Australian privacy principles(APP)**. It is illegal to conceal an incident, such as the exposure of a customer's health data, from consumers and the OAIC. That's why above statement is false.

6. You manage an organisation based in Australia, with an annual turnover of $20m, and you work closely with the European subbranches with a turnover of $10m. You have a number of staff working for you who deal with customer data on a daily basis. You have been sending direct marketing to your whole customer list, including those who have unsubscribed from marketing material. Your company is found to have violated a law and are fined $120,000.

Answer 6: this statement is true.

Organizations are not authorized to send direct marketing to clients who have already unsubscribed to the marketing field under the Australian privacy principles (APP) number 7. Continuing to send them direct marketing is tantamount to harassing the consumer, which is a criminal offence. As a result, the above sentence is correct.

7. You have found an interesting computer program online and download it. You make a back-up copy in line with the license terms. You have not committed any offences.

Answer 7: this statement is true.

Because downloading and copying programs from the internet falls inside the conditions of the license, it is not a criminal under the any act. As a result, the above sentence is correct.

8. You are retained by a company to go through computer programs they own to correct errors and test for security issues. You have not committed any offences.

Answer 8: this statement is true.

When you are hired by the company itself it is not a crime to test the company's own programs in order to rectify flaws and check the security of the system within the scope, since it is a part of ethical hacking or penetration testing. As a result, the above sentence is correct.