MODULE 3: DATA BREACH RESPONSE PLAN

In this exercise, you will work in small groups or individually to develop a data breach response plan for a fictional company.

Company Background:

CyberTech Solutions is a medium-sized IT consulting firm with 150 employees. They provide cybersecurity services like penetration testing, security audits, and incident response to clients across various industries. CyberTech handles sensitive client data including network diagrams, vulnerability reports, and some personal information of client employees.

Tasks:

1. Identify the key roles and responsibilities that should be part of CyberTech's data breach response team. Assign team member roles to your group.
2. Outline the 4 main steps CyberTech should take when responding to a data breach (contain, assess, notify, review). For each step, specify 2-3 key actions the response team should carry out.
3. Determine when CyberTech would need to notify the OAIC, affected individuals, and other third parties about a data breach under the Notifiable Data Breaches scheme.
4. Discuss additional sections or information that should be included in CyberTech's comprehensive data breach response plan.

Output:

Each group should prepare a maximum 600-word written summary outlining their data breach response plan for CyberTech Solutions. The summary should cover the main points addressed in the tasks above.

This exercise allows you to apply the concepts from Module 3 by developing a practical data breach response plan. It covers key elements like the response team, core response steps, notification requirements, and plan documentation. You will reinforce your understanding through discussion and collaborative work.