Delegate Name: Aamina Junaid Mohiddin

Country: Australia

Institution: Azzan bin Qais international school

Topic: Assessing and Mitigating the Dangers of Cyberattacks

“A breach alone is not a disaster, but mishandling it is” -Serene Davis

Cyber risks that affect Australia are varied and include ransomware attacks and data breaches. Several well-publicized cyberattacks that attacked Australian companies and organizations in 2023 highlighted the necessity of aggressive cybersecurity measures. The answer to the question of how hazardous a cyberattack is possibly disastrous. And the issue is simply getting worse. The UN adopted a new global counter-terrorism program on cybersecurity and New Technologies in 2020 that supports Member States, international organizations, and regional groups in building assistance in creating and executing efficient solutions to the difficulties presented by the internet in the fight against terrorism.

Data breaches in Australia are on the rise, affecting 13 major companies in the past 4 years. Australia has a robust criminal justice system and law enforcement infrastructure to tackle an extensive array of cybercrimes. This covers a wide range of offenses related to computers and telecommunications, under parts 7.3, 10.6, and 10.7 of the Commonwealth Criminal Code Act 1995. They include getting or handling personal financial information dishonestly, online child abuse, computer intrusions, unauthorized modification or destruction of data, and the production and dissemination of dangerous software, such as ransomware and viruses. Suspects who are suspected of committing cybercrime are charged under the criminal code, which is applicable throughout Australia’s states and territories. The government of Australia has introduced a blueprint that it describes as “game-changing” in order to safeguard the nation against an increasing amount of cyberattacks, the plan was unveiled in Sydney by Clare O’Neil, the minister in charge of cyber security and home affairs. During the first two years of the new schedule, which runs through 2025, special emphasis will be placed on building a more cooperative attitude amongst major sectors of the national economy and better-coordinating efforts of the public and private sectors to fight against cybercrime. The total agreement increases the cyber security commitment made by Prime Minister Anthony Albansese’s Labor administration by 587 million Australian dollars to the AUS $2.3 billion they had promised until 2030.

The delegate of Australia believes that international governments should work together to create a culture that is cyber-ready by constantly scanning networks for threats, providing corrective actions, preparing thorough, continuous education and awareness campaigns as well as conducting exercises with employees on a regular basis to keep them informed about cyber threats and appropriate responses allowing them to be more diligent.

Bibliography:

1.<https://calibreone.com.au/>

2.<https://www.unaa.org.au/learn/australia-and-the-un/australia-and-un-security-council/>

3.<https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity>

4.<https://www.ag.gov.au/>

5.<https://iclg.com/jurisdictions/australia>

6.<https://asia.nikkei.com/Politics/Defense/Australia-announces-game-changing-cybersecurity-plan>

7. <https://www.upguard.com/blog/biggest-data-breaches-australia>